Barracuda Cloud Security Guardian

Data Protection and Security

Last Updated Fed 28-2019 • US 1.0 • Copyright 2019 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com

TABLE OF CONTENTS

Overview ---- 3

1. Product Security ---- 3

1. Data Center Standards and Protection ---- 3

2.1 Storage Facility Standards ---- 3

2.2 Data Access and Storage ---- 3

2.3 Locations ---- 4

Americas: ---- 4

3. Operations and Organizational Controls ---- 4

3.1 New Hires and Orientation ---- 4

3.3 Training ---- 4

3.4 Oversight ---- 4

Last Updated Fed 28-2019 • US 1.0 • Copyright 2019 Barracuda Networks, Inc. • 3175 S. Winchester Blvd., Campbell, CA 95008 • 408-342-5400/888-268-4772 (US & Canada) • barracuda.com

Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.

Overview

This document walks through security measures in place to protect customer data accessed by Barracuda Networks. This document includes a description of the facilities that process data by Barracuda Cloud Security Guardian Service and descriptions of operational and organizational controls enforced by Barracuda Networks.

1. Product Security

1.1 Barracuda Cloud Security Guardian Service

Barracuda Security Guardian is a comprehensive software platform for public-cloud security and compliance orchestration. It continually scans your infrastructure to detect misconfigurations, actively enforces security best practices, and remediates violations automatically before they become risks. In addition, it also helps secure network and application infrastructure in the cloud by deploying and managing cloud native security services or Barracuda offered security products. Cloud Security Guardian involves 2 different components:

Stack deployed in the customer infrastructure – we collect telemetry from the customer cloud infrastructure using a small instance in Azure or AWS and the data is transmitted via API calls over HTTPS secured connection. This stack then forwards telemetry to SaaS over an encrypted channel. In addition, all data is also fed into BRS for further use. The stack has no inbound access, only sends outbound data to CGG SaaS service.

SaaS service – The SaaS service consists of multiple micro-services, a web front end for the customer to access, auth-db, csg-core service and Barracuda Reporting Service. CSG SaaS front end is hosted in Azure, the CSG-core service is currently hosted in AWS and other services are common Barracuda services. These services communicate amongst each other over a secure API channel.

1. Data Center Standards and Protection

2.1 Storage Facility Standards

Barracuda Networks leases space in a number of Tier 3 & 4 datacenters worldwide. Each Barracuda Networks datacenter is equipped with:

- Controlled access systems requiring key-card authentication.
- Video-monitored access points
- Intrusion alarms
- Locking cabinets
- Climate Control systems
- Waterless fire suppressant systems
- Redundant power (generator backup, UPS, no single point of failure)
- Redundant Internet connectivity

2.2 Data Access and Storage

Barracuda CSG does not store any customer data or PII. It reads customer infrastructure telemetry and shares it securely over an encrypted channel to the SaaS solution. For the infrastructure telemetry data, we store data in BRS and in elastic search hosted in AWS. Access to view the logs for debugging is restricted to Barracuda corporate networks.

Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.

2.3 Locations

The primary storage location for the Barracuda Cloud Security Guardian Service is as set forth below. Data is stored in the regions listed below and will not be stored or failed over outside the region in which the customer has set up the corresponding Barracuda product or service for which CSG has been enabled.

Americas:

- AWS Region - US East
- AWS Region - US West
- AWS Region – US Central

3. Operations and Organizational Controls

Barracuda Networks employees are expected to be competent, thorough, helpful, and courteous stewards of customer email that is stored on Barracuda Networks products and in Barracuda Networks datacenters. Barracuda Networks has established a number of measures to ensure that customers and their data are treated properly.

3.1 New Hires and Orientation

All new employees are required to accept and acknowledge in writing Barracuda Networks' policies for non-disclosure and protection of Barracuda and third-party confidential information, including acceptable use of confidential information. In the course of assisting customers with their technology solutions, Barracuda support technicians understand that they may come into contact with customer communications and/or customer data and they are not to view the contents of that data without explicit permission from the customer. Barracuda Networks employees are not to disclose the contents of that customer data to a third party under any circumstances.

New technical support employees are provided a job description and expectations when hired regarding maintaining the confidentiality and security of customer data.

3.3 Training

Technicians who support Barracuda Cloud Security Guardian Service are prepared in a variety of ways. New tier 1 technicians receive class time training with tier 2 technicians and the support management team. New support technicians also spend a period of time as understudies to an established technician for each product in which they intend to become certified.

All Barracuda Networks support technicians receive ongoing training in product-specific training sessions.

3.4 Oversight

Access to Barracuda Email Security Service servers is limited to approved Barracuda Networks personnel on an 'as needed' basis. Each tier 1 technician is attended by and reports to a tier 2 technician. Each tier 2 is responsible for no more than four tier 1 technicians. Support for Barracuda Email Security Service is provided from all our support regions. Support calls from customers in the United States are generally handled by technicians in the United States. Support calls from customers outside the United States could be routed to any of these facilities. When an employee or contractor leaves Barracuda, a formal process is in place to immediately revoke physical and network access to Barracuda Networks facilities and resources.

Barracuda Networks and the Barracuda Networks logo are registered trademarks of Barracuda Networks, Inc. in the United States. All other names are the property of their respective owners.