Barracuda Advanced Threat Protection

Data Protection and Security

TABLE OF CONTENTS

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 Advanced Threat Protection Service and descriptions of operational and organizational controls enforced by Barracuda Networks.

1. Product Security

1.1 Barracuda Advanced Threat Protection Service

Barracuda Networks offers a variety of security products that can utilize the BATP service which currently include our Next Gen Firewalls, Web Application Firewalls, Email Security Service, Web and Email Security Gateways. Each of these products offer methods for the administrator to control which types of files that are submitted to the service for analysis. Before a file can be submitted for evaluation there is a process for the security product to verify entitlement to the service by communicating with our license servers. Once validated the security product has permission to query BATP service for known samples and send files for analysis which are not yet known. In instances where a file must be sent for full sandbox emulation, BATP receives only the egress IP address, the product type from which it was sent, and the file for scanning. All communication between BATP and the security product is SSL encrypted, including transport of the file itself.

2. 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

Personal information is not accessible by BATP, it only maintains 4 key pieces of information about the file submitted including the file name, scan result, a unique hash id and meta data. Files that have been detonated in the sandbox and deemed clean are deleted immediately after scan is complete and report is generated. Virtual environments used for detonation are reset after each scan eliminating any trace of and therefore any access to the file. In cases where files are deemed malicious, Barracuda may maintain copies of those files to further improve security and train machine learning systems. Any files stored are kept in secure locations, accessible only by our threat research team, partner organizations, and engineering staff with directly applicable job requirements to access files. In every case, rigorous technical and security controls are in place to protect these files and systems. All computer systems exist in protected data centers that utilize both physical and electronic access controls, all access is monitored and audited.

2.3 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 Advanced Threat Protection 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:

- AWS Region - US East
- AWS Region - US West
- AWS Region - Canada

EU:

- AWS Region – Germany
- AWS Region - Ireland

APAC:

- AWS Region - Japan
- AWS Region - Singapore
- AWS Region - Australia

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 Customer Access to Data

Customers have no access to directly interact with BATP service, only the individual security product can interact with BATP as configured by the administrator of that product. Within each security product, only authorized administrators of the system have access to the analysis reports or any information that could tie specific samples back to end users. General information would include the file name, file type, scan determination, and time of scan. Some of this information presented within the product interface could be considered personal however, even in these cases the information presented in conjunction with the reports is limited to specific details that would assist the administrator in isolating and remediating the infected user or machine.

3.2 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 Advanced Threat Protection 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 Advanced Threat Protection Service servers is limited to approved Barracuda Networks personnel on an 'as needed' basis. The management team checks the status of support personnel through periodic ticket review and call monitoring. 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 Advanced Threat Protection 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