Barracuda Sentinel and Forensics Incident Response

Data Protection and Security

TABLE OF CONTENTS

Overview

This document walks through security measures in place to protect customer data accessed by Barracuda Network. This document includes a description of the facilities that process data by Barracuda Sentinel and Forensics Incident Response (Forensics) for the descriptions of operational and the organizational controls enforced by Barracuda Networks

1.Product Security

1.1 Barracuda Sentinel and Forensics

Barracuda Sentinel is a multi-layer AI engine that detects and blocks spear phishing and socially engineered attacks in real time and identifies which employees are at highest risk.

Barracuda Forensics is a SaaS solution that lets your IT team identify, track and resolve email attacks from outside your organization.

Barracuda Sentinel and Forensics integrate directly with Microsoft Office 365 API to secure data transfer using TLS 1.2 or higher HTTPs connection.

2.Data Transmission and Storage

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 Storage

Barracuda Sentinel and Forensics transmit the data from the customers O365 server to Barracuda cloud. Once received the data is indexed and stored using AES 256-bit encryption in our secure AWS VPC environment.

Data Locations

The primary storage location for the Barracuda Sentinel and Forensics is as set forth below: Data is stored in the region 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 Barracuda Sentinel and Forensics has been enabled.

US

- AWS Region - US East - 2

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 email without explicit permission from the customer. Barracuda Networks employees are not to disclose the contents of that customer email 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 email.

3.2 Training

Technicians who support Barracuda Sentinel Forensics 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.

3.3 Oversight

Access to Barracuda Email Sentinel and Forensic 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 Sentinel and Forensics 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.