Barracuda Managed Workplace

Protection and Security

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 Managed Workplace Service and descriptions of operational and organizational controls enforced by Barracuda Networks.

1. Product Security

1.1 Barracuda Managed Workplace Security

Managed Workplace is a complete remote monitoring and management (RMM) platform with robust, integrated security tools and services. With Managed Workplace RMM, IT service providers can quickly assess vulnerabilities, secure weak points, monitor anomalies, and seamlessly recover data in the event of an attack – all from a single dashboard. Managed Workplace solution is a SaaS solution that runs on Public Cloud in Amazon Web Services (AWS).

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, Transmission and Storage

Partners can configure user roles and permissions to define the level of access users have to the Service Center. In addition to using standard usernames and passwords to login into Service Center, partners can enable Multi-Factor Authentication (MFA) and/or Single Sign-On (SSO) for added protection. Each login access to Service Center is recorded in an audit log that the partner can access. Only select individuals from the Managed Workplace Operations, Engineering and Support teams can access our AWS cloud. Employees access the clouds use the Remote Desktop Protocol (RDP) and must enter Active Directory (AD) credentials to gain access.

Onsite Managers and Device Managers use TLS to communicate to Service Center. TLS is an industry standard protocol that provides 3 services to applications: encryption, authentication and data integrity. Zero firewall adjustments are needed on the client side to send data to the Service Center. The Onsite Manager or Device manager will initiate an outbound connection over the standard TLS port (443). Similarly, only port 443 is allowed inbound to the Service Center servers. This is locked down by traditional firewall and by AWS security groups.

Sensitive data including Service Center login passwords and credentials used to monitor and managed devices are encrypted by Service Center using strong algorithms including bcyrpt and AES before being stored.

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

The primary storage location for the Barracuda Managed Wrokplace 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 Managed Workplace has been enabled

Americas:
AWS Region - US East
AWS Region - US West

EU:
AWS Region - Germany

APAC:
AWS Region - Australia

3. Operations and Organizational Controls

Barracuda Networks employees are expected to be competent, thorough, helpful, and courteous stewards of customer data that is stored on Barracuda Networks products and in Barracuda Networks data centers. 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.

3.2 Training

Technicians who support the Barracuda Managed Workplace are prepared in a variety of ways.
New technicians receive class time training with senior technicians and the support management team. New support technicians also spend a period of time as an understudy 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 Managed Wrokplace 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.

Support for Barracuda Managed Workplace is provided out of United States and Canada. Support calls generally start in the United States with a Tier 1 representative but may get escalated to a Tier 2 or 3 representative in Canada if necessary.

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.