Remote Monitoring and Management SaaS Service Description

Barracuda sells the Service to managed service providers ("**MSP**") for their use in connection with the managed services the MSP provides to its end customers. Such sale and use of the Service is subject to this Service Description and the MSP's agreement with Barracuda under which the MSP purchases the Services. If an MSP provides its end customers with access to the Service, it must pass through to its end customers the Barracuda Customer Terms and Conditions.

The applicable governing terms and conditions document and this Service Description together are referred to as the "**Agreement.**" This Service Description will govern if there is any conflict with other documents. References to the "end customer" means the MSP's end customer that uses or benefits from use of the Service. Any capitalized terms used but not defined below have the meanings in the Agreement.

Overview

The Service is a turnkey, security-centric remote monitoring and management SaaS tool that provides a built-in security assessment to enable MSPs to quickly assess the security of their end customers' networks, deliver multi-layered security services, monitor anomalies, and seamlessly recover data within the Service in the event of an attack. Customers may purchase separately from Barracuda a license to software from SentinelOne that is installed on end customer devices and a Barracuda cloud-based management consol called the Service Center. The client software transmits information to the Service Center.

This Service Description applies to the Barracuda hosted version of the Service. MSPs may host their own instance of the Barracuda software in their own environment. This Service Description does not apply to self-hosted instances of the Barracuda software. MSPs are responsible for self-hosted versions of the software, including obtaining rights to use and distribute SentinelOne or other compatible end point detection software. MSPs are also responsible for the data that the MSP collects and uses through that self-hosted platform, including responsibility under applicable data handling and privacy laws. MSPs who self-host the Barracuda software must hold Barracuda harmless from their acts and omissions in connection with that activity.

Unit of Measure and Limitations

The Service is licensed by the *number of licenses per physical device managed by the Service*. Use of the Service is limited to the number of invoiced licenses.

Overuse. If an MSP uses the Service beyond the number of invoiced licenses, then Barracuda will notify the MSP so that it can bring its use within the invoiced license limit to avoid additional charges. If the MSP is not able to bring its use within the invoiced license limit within 60 days of the date of Barracuda's notice, then Barracuda may send the MSP a further invoice for the over-use at the then-current list price. The MSP agrees to pay the additional invoice upon receipt.

End Customer Systems. MSP represents that it has obtained the necessary authorizations to provide the Service for the networks, systems, IP addresses, assets, and/or hardware (collectively "Devices") including those that it targets, scans, monitors, or tests using the Service, and to collect data, including log data, from Devices.

End Customer Access to the Service. If an MSP uses the Service for more than one end customer, and the MSP provides access to the Service to any end customer, then the MSP must ensure that the settings for the Service allow each end customer with access to the Service to see only its data in the Service and not the data of any other end customer. Before an MSP provides access to the Service to an end customer, the MSP must notify Barracuda of the name of the end customer, its physical address, and such other information that Barracuda may need to conduct trade compliance screening of that end customer so that Barracuda can comply with its legal obligations under applicable trade laws.

Data Privacy

Global Data Processing Addendum (DPA)

Barracuda's DPA provides both Barracuda's and its customers' rights and obligations regarding the processing of Customer Personal Data (as defined in the DPA) in connection with Barracuda's products and services. Barracuda's customers can electronically execute the DPA via our Trust Center. For more information about how Barracuda processes personal data as a data controller, please review our Privacy Notice.

Cross-Border Data Transfer

As a global company, Barracuda operates worldwide. When Barracuda receives or transfers personal data from the European Union, the UK, or Switzerland it does so in accordance with GPDR and local data protection laws. Where required, Barracuda leverages European Commission approved cross-border data transfer mechanisms including the EU's Standard Contractual Clauses incorporated into our DPA. For data transfers to the United States, Barracuda is self-certified under the US Department of Commerce Data Privacy Framework, and its certification can be found here.

Data Retention

The Service collects and stores information, including credentials, accounts, endpoint device information (e.g., IP addresses, device health information), as well as user account data. Although the Service is set to store data for 120 days as a default, MSPs can change the data retention parameters within the Service management console ("Service Center").

If an MSP's end customer is removed from the Service, then all information about that end customer will be purged from the database within approximately 2 weeks unless Barracuda encounters technical issues.

If an MSP has been removed from the Service, then Barracuda will commence deleting the MSP's data no later than 120 days. Some deletion activities may occur sooner.

Location of Customer Data

Please see the *Security – Data Storage* section below for information about where customers may store their data.

Data Transmission

Data is encrypted in transmission and at rest.

Access Control

MSPs may configure remote controls and roles for end customers through the Service Center. More information of this feature can be found at the following address: https://campus.barracuda.com/product/managedworkplace/doc/171942529/configuring-remote-control-for-end-user.

Security

Data Transmission and Storage

Storage Facility Standards

Barracuda Networks leases space in an AWS data center. The data center 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

Data Storage Locations

The storage location for data used for the Service is as set forth below. MSP and end customer data will not be stored or failed over outside the region in which the MSP has set up the corresponding Barracuda product or service for which the Service has been enabled.

Americas

- AWS Region – North America

Europe

- AWS Region – Frankfurt

Australia

- AWS – Australia

Operations and Organizational Controls

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

New Hires and Orientation

All new employees are required to accept and acknowledge in writing Barracuda's policies for non-disclosure and protection of Barracuda and third-party confidential information, including acceptable use of confidential information. When 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 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.

Training

Technicians who support the 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 time as understudies to an established technician for each product in which they intend to become certified. All Barracuda support technicians receive ongoing training in product-specific training sessions.

Oversight

Access to the Service is limited to approved Barracuda personnel on an 'as needed' basis. Each tier 1 technician is attended by and reports to or is mentored by a tier 2 or tier 3 technician. Each tier 2 or, when applicable, tier 3, is responsible for no more than four tier 1 technicians. Support for the 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 facilities and resources.

Use of Artificial Intelligence

The Service does not use Artificial Intelligence. (AI)

The Service is not intended for use in situations that would cause the Service to be considered "High-risk AI" under the EU AI Act. MSPs must not use the Service in a manner that would subject Barracuda to obligations applicable to High-risk AI. Barracuda may terminate the customer's applicable subscriptions to the Service if it violates this obligation. Barracuda has no responsibility for customers' use of the Service in situations considered "High-risk AI."

Data Export

The Service includes the RMM Data Warehouse where Barracuda stores the MSP's end customer data (segregated by MSP). The data from the Service Center automatically syncs to the RMM Data Warehouse. When the Service is installed, access to the RMM Data Warehouse is not enabled. MSPs must request access.

MSPs must not provide access to the RMM Data Warehouse to its end customers because that would allow an end customer to see other end customers' data. MSP is responsible to Barracuda for any breach of this restriction.

MSP personnel with access to the RMM Data Warehouse may export that data to run reports for their respective end customers. MSP's end customer data stored in the RMM Data Warehouse can only be accessed by MSP personnel with an administrative role and permissions.

Back Ups and Disaster Recovery

For Barracuda's AWS environment, Barracuda maintains a comprehensive data backup policy to support business continuity and disaster recovery best practices. Data backups are taken on a daily basis. In the event of a wide-scale service outage, Barracuda will work with impacted Customers.

Service Level Agreement ("SLA")

There is no SLA for this Service.

Barracuda Trust Center

The Barracuda Trust Center is located at https://trust.barracuda.com/. Barracuda periodically updates the Trust Center. The then-current version of the Trust Center governs.

At the Trust Center customers can find the following, among other information:

- Product Certifications : https://trust.barracuda.com/security/certifications
- Security advisories: https://trust.barracuda.com/security/information#security-advisories
- Trade Compliance information and certain applicable forms: https://trust.barracuda.com/legal/trade-compliance
- Frequently requested documents, such as Certificate of Insurance, Business Associate Agreement, Non-disclosure Agreement, copy of the current SOC2 report, privacy documents, and more.

MSP-provided Third Party Software

In situations where the MSP wishes to use third party software to interoperate with the Service, MSP grants Barracuda permission to allow the third party and its provider to access Customer Data and information about MSP's usage of the third party product or service as appropriate for the interoperation of that third party product or service with the Service. MSP is responsible for ensuring that it has sufficient rights under applicable law to such third party software to grant the rights to Barracuda to allow Barracuda to perform its obligations for the MSP.

Barracuda-provided Third Party Software

Barracuda provides SentinelOne software for use with the Service and is required to flow through the provider's terms. MSPs who purchase these Services from Barracuda for use in providing services to their end customers can view the SentinelOne terms at the following address:
https://assets.barracuda.com/assets/docs/dms/XDR_Third_Party_Flow-down_Terms-MSPs.pdf

Discontinuation of the Product

Barracuda will provide distributors, resellers and other customers reasonable advance notice before discontinuing the sale of the Service (or associated material functionality) unless Barracuda replaces such discontinued Service or functionality with a materially similar Service or functionality. Nothing in this section limits Barracuda's ability to make changes required to comply with applicable law, address a material security risk, or avoid a substantial economic or material technical burden. This section does not apply to pre-general availability Services, offerings, or functionality.