Barracuda Message Archiver Product Description

Barracuda sells products and services through channel partners to end users that use the products and services in their own business. For customers that purchase the Barracuda Message Archiver product ("**Product**") from a Barracuda authorized channel partner, your use of the Product is subject to this Product Description and the Barracuda Customer Terms and Conditions (unless you have a negotiated agreement with Barracuda, in which case the negotiated agreement will apply).

Barracuda also sells the Product 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 Product is subject to this Product Description and the MSP's agreement with Barracuda under which the MSP purchases the Product. MSPs pass through to their end customers the Barracuda Customer Terms and Conditions (which incorporate this Product Description).

The applicable governing terms and conditions document and this Product Description together are referred to as the "**Agreement.**" This Product Description will govern if there is any conflict with other documents. Customers that purchase from an authorized channel partner and MSPs who purchase the Product are collectively referred to as the "**Customer**." References to the "end customer" means the entity that benefits from use of the Product, regardless of purchasing methodology. Any capitalized terms used but not defined below have the meanings in the Agreement.

Overview

The Product is ideal for organizations looking to reduce their email storage requirements and boost user productivity with desktop access to any email ever sent or received.

Data is archived outside the customer's operational email environment in a dedicated tamper-proof repository, ensuring it will be retained securely for as long as it is needed. The Product's policy-based approach uses granular retention policies to allow customers to retain data securely for as long as it is needed.

The Product is available as a physical appliance or as an integrated virtual solution for on-site or in-the-cloud deployment. Customers can purchase the Product and configure the virtual appliance directly in AWS, or install locally on VMware or Hyper-V.

Unit of Measure and Limitations

The physical appliances are sold per appliance. The software on the appliances supports the capabilities of the hardware, so if a customer reaches the capacity of the hardware, then the Customer must upgrade to hardware with larger capacity and purchase a subscription to the applicable software. Software on the physical appliances is licensed under a subscription for an agreed period, either monthly or one or more years. At the end of the subscription, the license to software expires and Customer must stop using it. Without the software subscription, the Product will not receive any further software (including firmware) updates.

For virtual machines, the software is made available as an Amazon Marketplace Image (AMI) for deployment in Customers' AWS environments. Once deployed, the unit of measure and space constraints are the same as for physical appliances. If a customer uses a virtual machine up to the license capacity purchased, then the customer must purchase a higher-capacity virtual machine package. Using a virtual machine beyond the license capacity purchased is a violation of the license and the Agreement.

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

Customers control the data retention policies and practices for both the physical and virtual appliances.

Location of Customer Data

Customers determine where they place the Product – on their premises or for virtual appliances, in the customer's data center or the customer's tenant on AWS. For customers who chose the AMI (virtual) instance for the Product, that data is stored in the customer-chosen region. The Security section below identifies the data centers at which Customer data may be stored.

Security

Barracuda Physical and Virtual Appliance Security

The Product is typically deployed behind the customer's corporate firewall and is protected by the same security that the customer uses to protect primary data sources. There are several ways the Product can be accessed locally, and each is dedicated to a specific function:

- The local web interface provides access for appliance configuration and all product functionalities.
- A monitor and keyboard provide access to the terminal configuration for network setup and troubleshooting. Command-line access to the unit is disabled locally.

The Product runs on a hardened Linux kernel. If a security flaw is discovered, updates are pushed out to the Product in a security definition administered by Barracuda.

Data Locations

The virtual appliance version of the Product is offered as an AMI for AWS EC2 on AWS . Customers may choose one of the following AWS locations to deploy their virtual appliance:

Americas:

- U.S.: infrastructure deploys in this region stores data for all customers in the United States, as well as any region not specifically configured to send data to an available local location.
- Canada: stores data for all customers in Canada.

EMEA:

- United Kingdom: stores data for all customers in the United Kingdom, Europe, Middle East and Africa.
- Germany: stores data for all customers in Germany, Austria, Belgium, Netherlands, and Luxembourg.

APAC:

- Australia: stores data for all customers in Australia.

Access Control & Security Recommendations

Barracuda Physical and Virtual Appliance Access Controls

The Product provides the following features to control access to the Product:

- Customers can configure multiple user roles to determine the level of access to the functionality of the Product. More information about this feature is available here: https://campus.barracuda.com/product/messagearchiver/doc/2490376/how-to-manage-user-accounts-and-roles
- IP login restrictions can be set for administrative users of the Product. Those restrictions prevent access to the web user interface from an IP address outside the range specified.

Technical support for the Product employs the Barracuda support tunnel service to allow an authorized technician to directly access the unit. Access to the Product is only possible when the Customer consents to that access by opening the support tunnel.

User access to the support tunnel service is limited to Barracuda authorized support and engineering personnel. Regular access control audits are conducted to ensure that only authorized personnel are allowed to access the system. All activity performed on Customer units is logged to a central logging system monitored by Barracuda's Security Team. Logs of activity are maintained for 90 days.

Operations and Organizational Controls

Barracuda has established several 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 with a job description and expectations when hired regarding maintaining the confidentiality and security of customer data.

Training

Technicians who support the Product 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 Product 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 Product is provided from all Barracuda 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.

Support

Barracuda offers the following support pursuant to the Barracuda Technical Support Policy:

- Instant Replacement subscription.
- Enhanced or Premium Support subscription

Use of Artificial Intelligence

The Product is not intended for use in situations that would cause the Product to be considered "High-risk AI" under the EU AI Act. Customers must not use the Product in a

manner that would subject Barracuda to obligations applicable to High-risk AI. Barracuda may terminate the customer's applicable subscriptions associated with the Product if it violates this obligation. Barracuda has no responsibility for customers' use of the Product in situations considered "High-risk AI."

The Product does not include the use of artificial intelligence.

Back Ups and Disaster Recovery

The Products offer a backup feature where Customer can manage and store their own back-ups on a location of their choice.

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.

Customer-provided Third Party Software

In situations where Customer wishes to use third party software to interoperate with the Product, Customer grants Barracuda permission to allow the third party and its provider to access Customer Data and information about Customer's usage of the third party product or service as appropriate for the interoperation of that third party product or service with the Product. Customer 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 Customer.

Discontinuation of the Product

Barracuda will provide distributors, resellers and other customers reasonable advance notice before discontinuing the sale of the Product (or associated material functionality) unless Barracuda replaces such discontinued Product or functionality with a materially similar Product 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 Products, offerings, or functionality.