Your business, secured.

Email Security Gateway 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 Email Security Gateway 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 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.

End of Sale

As of June 3, 2024, this Product in both physical and virtual appliance forms is no longer available for sale to new customers ("**End of Sale Date**"). Customers cannot migrate to a higher level of the Product. Barracuda's successor offering is Email Gateway Defense. Customers who purchased the Product and a subscription to Instant Replacement before the End of Sale Date may renew that subscription in 1-year increments. **Barracuda has not declared an end of support or end of life date for the Product. The company continues to provide technical support to customers who have the Product before the End of Sale Date and who have continuously maintained their Energize Updates subscription.** Barracuda technical support includes provision of critical security patches and firmware updates for supported versions of firmware as well as answering technical questions and helping customers troubleshoot issues. Customers who let their subscription to Energize Updates lapse will lose access to technical support, including security updates, and will not be allowed to subsequently renew their subscription.

Overview

The Product protects customer email environments by pre-filtering every inbound and outbound email before delivery using virus scanning, spam scoring, real-time intent analysis, URL link protection, reputation checks, and other techniques. The Product includes a secure email gateway combined with threat intelligence updates that include new security definitions to blocks multiple types of email threats, eliminating the need for separate email and data protection solutions.

The Product can be deployed at the customer's physical locations as hardware or virtual appliance. Customers can deploy virtual appliances in their cloud tenant in Microsoft Azure, AWS, and Google cloud platforms. Each Product connects to a Barracuda cloud service through which the Products receive updates to software, including feature updates and updates to the firmware, including threat intelligence updates that include new security definitions.

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 only function in "demo mode" with a limited set of functions.

For virtual machines, the software is licensed by CPU Cores. If a customer uses a virtual machine up to the capacity of the CPU Cores purchased, then the customer must purchase a higher-capacity virtual machine package.

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 physical and virtual appliances.

Location of Customer Data

All data is held on the Products. Customer determines where they place the Products – on their premises or for virtual appliances, in Customer's data center or Customer's tenant in a cloud platform. Customer control placing data on and removing data from the Products.

Security

Barracuda Physical and Virtual Appliance Security

Barracuda physical and virtual appliances are closed systems: Barracuda provides all updates to the operating system and applications required to ensure the security and functionality of the product.

To ensure security of our products, Barracuda:

1. Implements strict change control processes during the development process.
2. Monitors security feeds to identify vulnerabilities that could affect product components.
3. Performs authenticated host and application level security scans prior to each firmware version release.
4. Exposes our products to continuous external security testing via our bug bounty program.

Product security issues are typically resolved via updates to currently supported firmware versions. Critical security issues are addressed, when possible, with targeted patches called Security Definitions. All customers with current support contacts are eligible to receive firmware updates and Security Definitions. However, to get security updates, customers must ensure their appliances are running a supported version. Customers in dark environments should contact support for guidance on applying firmware updates and security updates.

Access Control & Security Recommendations

Barracuda Physical and Virtual Appliance Access Controls

Customers can determine whether emails that pass through the Product are encrypted or are in plain text.

Technical support of Barracuda appliances can, at times, employ the Barracuda support tunnel service to allow an authorized technician to directly access the unit. Access to the device 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 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 our Security Team. Logs of activity are maintained for 90 days.

Security Recommendations

Security appliances sit in a privileged position in customer networks. Customers should take care to prevent unauthorized access to the administration interface. Administrative credentials should be stored securely and rotated when users with access to them leave the company or change roles.

Barracuda appliances ship with HTTP access to their management interfaces enabled. This should be considered a temporary solution while procuring and installing an official SSL certificate for the devices. Due to the requirements for generating such a certificate, Barracuda cannot perform this step for customers. Once a certificate is installed, the appliance should be configured to only allow access to the management interface over HTTPS. See product documentation for details.

Our products also have product specific controls that support limiting access to the administrative interface. Consult the product documentation and consider implementing the option to increase the security of your device – especially if the user interface is exposed to the public internet.

Operations and Organizational Controls

Barracuda employees are expected to be competent, thorough, helpful, and courteous stewards of customer data that is stored on the Product. 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 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 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

This Product does not employ 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.”

Back Ups and Disaster Recovery

The physical appliance version of this Product resided in a customer data center. The virtual appliance version resides either in a customer’s data center or in a customer’s cloud tenant. In all cases, customers are responsible for setting and implementing backup and disaster recovery policies.

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 the customer wishes to use third party software to interoperate with the Product, the 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 Service. 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 Support

Barracuda will provide distributors, resellers and other customers with reasonable advance notice before discontinuing support for the Product. 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.