Barracuda Email Protection SaaS Service 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 Email Protection SaaS service offering ("**Service**") from a Barracuda authorized channel partner, your use of the Service is subject to this Service 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 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. MSPs pass through to their end customers the Barracuda Customer Terms and Conditions (which incorporate this Service Description).

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. Customers that purchase from an authorized channel partner and MSPs who purchase the Service are collectively referred to as the "**Customer**." References to the "end customer" means the entity that benefits from use of the Service, regardless of purchasing methodology. Any capitalized terms used but not defined below have the meanings in the Agreement.

Introduction

The Service provides a comprehensive, cloud-delivered solution that combines email filtering and policy enforcement, advanced threat prevention, automated incident response, and domain fraud protection into a unified experience.

It leverages artificial intelligence and behavioral analysis to detect and block threats such as phishing, ransomware, and business email compromise. By continuously analyzing message content, links, attachments, and communication patterns, the Service identifies anomalies and prevents targeted attacks in real time.

When threats reach users, the Service automates investigation, containment, and remediation—enabling rapid response to reduce risk and minimize impact. As a SaaS offering, it simplifies ongoing security management and ensures continuous protection without requiring customer-side infrastructure or updates.

Unit of Measure and Limitations

The licensing metrics and associated restrictions for this Service are defined at: https://campus.barracuda.com/product/campus/doc/172891718/license-definitions-email-protection-products/

For MSPs that would like to use the Service to manage their internal business data, the MSPs must acquire a separate subscription to the Service. MSPs must not co-mingle their internal business data with the data of any customer in the Service.

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

Upon termination, Barracuda will retain customer data in the Service for up to thirty days to give customers the opportunity to download their data. After the thirty-day period, Barracuda will have no obligation to maintain or provide any customer data and will have no liability resulting from the destruction of the customer data.

Location of Customer Data

The Service stores customer data on Amazon Web Services (AWS) cloud infrastructure in the United States. See the Security section below for more information.

Access Control

Customers can manage access, permissions, and users manually or by integrating with directories via LDAP or Microsoft Entra ID.

Security

Data Transmission and Storage

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

Customer data transmitted through the Service is encrypted in transit and at rest using industry-standard encryption protocols. To ensure high availability and data durability, the Service stores and replicates data across multiple secure Barracuda-operated or -managed data center locations.This diverse storage system serves to further strengthen the physical security of customer email. With this architecture, the Service can maintain up to three distinct copies of customer data. Each of these copies is stored in the cloud.

Data Locations

The location of data storage and processing for the Service depends on the specific capabilities enabled.

- **Impersonation Protection and Incident Response (IP/IR)**

  Data is stored in the AWS region selected during the initial Service setup. Data will not be stored or failed over outside the customer-designated region. Current available region:

  - **United States** – AWS US East (N. Virginia)

- **Email Gateway Defense (EGD)**

  The cloud infrastructure for this component is deployed across multiple AWS regions. Data may be replicated within the selected region to support availability and durability. Current deployment regions include:

  - **United States** – AWS US East (N. Virginia)
  - **Canada** – AWS Canada Central
  - **United Kingdom** – AWS EU West (London)
  - **Germany** – AWS EU Central (Frankfurt)
  - **Australia** – AWS AP Southeast (Sydney)

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

This Service uses AI, including Barracuda's Advanced Threat Protection AI capabilities. The Service is not a "High -risk AI" application as defined in the EU AI Act. Below are some FAQs regarding that use.

- What is the data that is used to train the AI in this Service?
    - This Service uses AI to analyze the malicious emails ("Threat Data") from all customers to train its proprietary threat intelligence algorithm. The AI analyzes content of incoming messages in accordance with Barracuda's threat intelligence algorithm and then identifies known phishing patterns and signatures, allowing the Service to swiftly recognize and flag suspicious emails. Beyond known patterns, the AI looks for anomalies in email behavior and characteristics. It identifies irregularities in sender behavior, unusual email content, or deviations from established communication patterns. The model itself does not contain the personal information of anyone and instead reflects the patterns of malicious behavior that have been extracted from the Customer Data.

- Does Barracuda regularly refresh the Threat Data used to train the model?
    - Yes. Barracuda refreshes the Threat Data regularly so that the model constantly learns about the latest threats that customers face. Barracuda's AI model continually learns and adapts to new threats. As new Threat Data becomes available, its models and heuristics are automatically updated to improve the accuracy of detection.
- Where does Barracuda store the Threat Data used to train the model?
    - Barracuda stores the Threat Data in its tenant on AWS in the United States.
- Does Barracuda remove personal information from the Threat Data before the Threat Data is used to train the model?
    - No, because that information is analyzed to understand the pattern of the malicious behavior. That said, personal information is not used other than to understand the malicious behavior. Personal information does not become part of the model.
- Do other products also use this Threat Data set?
    - No. Other products will use the AI models that have been trained on the Threat Data, but they do not use the Threat Data set itself.
- Does the Service use generative AI? o No

Data Export

This Service does not archive or store data on Customer's behalf.

The Service allows customers to export its data at any time.

Back Ups and Disaster Recovery

For Barracuda's AWS environment, the company maintains a comprehensive data backup policy to support business continuity and disaster recovery best practices. Data backups are taken daily.

Service Level Agreement ("SLA")

The Service includes multiple capabilities. Service Level Agreements apply only to specific components as stated below. Barracuda publishes Service status updates at: https://status.barracuda.com.

- **Impersonation Protection and Incident Response.** These capabilities **do not include a service level agreement** for uptime or availability.
- **Email Gateway Defense.** Barracuda offers the following SLA commitments to customers with a paid subscription to the Email Gateway Defense SaaS application (excluding free trials and suspended accounts):

    1. **Email Delivery Commitment.** Subject to the Exceptions in section 3 and the exclusions listed below, Customers will be able to send and receive email through Barracuda's email servers **at least 99.9% of the time** during each calendar month.

        This commitment excludes:

        - Emails with encrypted or password-protected attachments
        - Emails subject to complex full-text content policies
        - Bulk emails to large distribution lists (which may be serialized)
        - Customer or third-party internet failures
        - Customer-induced viruses
        - Non–RFC-822-compliant mail servers
        - "Open relay" server configurations

    2. **Web Uptime Commitment** Subject to the Exceptions in section 3 below, Customers will be able to access the Email Gateway Defense management console **at least 99.9% of the time** during each calendar month,
    3. **Exceptions**. The above commitments are subject to the following exceptions: (a) planned downtime or emergency maintenance for the Service; and (b) any unavailability caused by: force majeure event; actions/inactions by persons other than Barracuda and its contractors; third-party products or services used with the Service; outages that are less than 5 continuous minutes in duration (e.g., monitor connectivity glitches); Internet, hosting or platform service provider failure or delay; denial of service attack; use of the Service in violation of the Barracuda Customer Terms and Conditions; or use of Service

that is not in accordance with Documentation (as defined in the Customer Terms and Conditions) (collectively "**Exceptions**").

Service-impacting conditions must be reported to Barracuda Support within 24 hours of that event. If required, customers must also grant access to their Service account and any related on-premises Barracuda equipment. Downtime calculations begin once the issue is reported.

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.

Discontinuation of Service

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.