BarracudaONE Service Description

The BarracudaONE Service ("**Service**") maximizes customer protection and cyber resilience by unifying cybersecurity solutions in a centralized dashboard. The Service simplifies and strengthens customer security operations by consolidating the management of multiple solutions into a single, unified Service, eliminating the need for multi-vendor solutions and the hassles that go with managing them. With AI-powered layered threat protection in the products and services accessible through the Service, the Service reduces operational complexity. By consolidating key security functions, the Service minimizes customers' administrative burden, providing improved visibility, reducing risk and simplifying operations. The Service is currently available to Barracuda customers without additional charge.

For customers that purchase directly from Barracuda or 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). If there is a conflict between those documents, this Service Description will prevail.

Barracuda API Portal

The BarracudaONE API Portal provides customers and partners with secure, programmatic access to selected BarracudaONE platform data and capabilities. Through documented REST-based APIs, authorized users can integrate BarracudaONE with third-party systems such as SIEM, SOAR, IT service management, and reporting tools, enabling automated data retrieval, workflows, and operational insights. Access to the API Portal is governed by scope-based permissions and authentication controls to help ensure data security and appropriate use. The APIs are designed to support common operational and reporting use cases while maintaining the same security and compliance standards applied across the BarracudaONE platform.

Data Protection

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

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 personal 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 does not ingest or otherwise collect customer data or customer Personal Data, except as needed for customers to register for and use the Service. When a customer subscribes to a Barracuda product, that product will send information to the Service about customer use of products. The Service uses that information to create value reports for the customer. The Service keeps customer value reports for a rotating six-month period. Older reports are deleted. Customers can download these reports any time before they are removed from the Service.

Location of Customer Data

The Service is offered on the AWS cloud infrastructure : US East (Ohio)

Access Control

The Service provides Admin and non-Admin roles. For MSP customers, individuals have Admin role access if they also have Admin role privileges within the Barracuda MSP App. For all other customers, the Service uses the same Admin privileges that the customer established in the customer's Barracuda Cloud Control account.

Security

Data Transmission

The data used to create the customer value reports is stored in a Barracuda cloud data lake on AWS in the United States where it is encrypted at rest. The information is encrypted in transit when sent to the Service. Once the Service uses the product usage data to create the value report for the customer, the data is removed from the Service.

Operations and Organizational Controls

Barracuda employees are expected to be competent, thorough, and helpful. 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.

Barracuda AI Services

At Barracuda, artificial intelligence ("AI") is essential to our business, helping us improve product development and strengthen automated threat detection and cybersecurity services. We rely on curated AI technologies including machine learning, deep learning, generative and agentic AI, as well as select third-party AI solutions—all of which we refer to as "Barracuda AI Services".

Barracuda AI Services enables responsible AI innovation that safeguards our customers against advanced cyber threats and drives our business.

Barracuda AI Services enhance customer experiences and support Barracuda products and services that protect our customers and their data. Barracuda AI Services are only provided in conjunction with other Barracuda products or services.

Barracuda AI Services are deployed in various ways depending on the product or service supported. These use cases include, for example:

- Multi-modal AI and advanced machine learning to identify anomalies and threat indicators including suspicious IP addresses, QR codes with dangerous links, malicious intent, files containing malware, etc.
- Machine learning and deep learning technology leveraging curated threat intelligence engineered to detect indicators of compromise and quarantine threats in real time.
- Barracuda Assistant – Powered by Barracuda AI is a generative AI chat experience designed to support Barracuda customers and partners while using and engaging with our products and services.

No High-Risk AI Systems

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 use of the Service if it violates this obligation. Barracuda has no responsibility for customers' use of the Service in situations considered "High-risk AI."

Termination and Data Export

If a customer stops using a Barracuda product, then data about the customer's use of the product will stop being transmitted to the Service. Six months after the customer stops using a Barracuda product, all value reports will be removed from the Service. Customers must export any value reports they want to keep before that time.

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 a customer wishes to use third party software to interoperate with the Service, 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. The 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 Service

Barracuda will provide distributors, resellers and other customers reasonable advance notice before discontinuing availability of the Service. 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.