Advanced Threat Protection
Service Description

Overview

Barracuda includes some or all of the elements of Advanced Threat Protection Services (ATP Service) in many of its Products and Services. ATP Service comprises various layers of protection within a suite of software tools. ATP Service is only available when purchased or included with other Barracuda Products or Services.

ATP Service, which may leverage components of Barracuda AI, analyzes email, files, and network traffic for known indicators of compromise and neutralizes threats before they can reach our customers.

Barracuda AI

Barracuda AI comprises advanced artificial intelligence technologies, including machine learning, generative and agentic AI, and curated AI solutions. This technology foundation supports Barracuda's intelligent business operations, AI-enhanced development, automated threat detection, and cybersecurity services. Engineered on a robust and secure infrastructure, Barracuda AI enables responsible AI innovation that safeguards our customers against advanced cyber threats and drives our business.

The ATP Service uses Barracuda AI to analyze and detect threats. ATP Service uses 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.

Barracuda AI processes Systems Data including Threat Data and Threat Intelligence. Refer to the Barracuda Legal Terms and Conditions for the full definition of Systems Data.

- *Threat Data* is unfiltered data used to differentiate between normal and malicious behavior and content.
- *Threat Intelligence* is information from multiple sources that Barracuda has curated and enhanced to train and inform our models. It includes Threat Data.

Barracuda AI learns from Threat Data elements including emails, files, and other information processed via Barracuda products and services. Regular and relevant Threat Data ingestion keeps Barracuda AI current to protect customers against threat actors and cyber criminals in real-time. Threat Data is parsed and enhanced within Barracuda AI to develop Barracuda Threat Intelligence. This data informs our algorithms and systems to accurately distinguish

between abnormal and normal, expected patterns and data. This is essential for improving efficacy and identifying threat indicators that may signal a cyber risk.

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. Customers can electronically sign 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 Transfers

When Barracuda receives or transfers personal data from the European Union, the UK, or Switzerland it does so in accordance with GPDR and other relevant data protection laws. Barracuda uses European Commission-approved cross-border transfer mechanisms, including the EU's Standard Contractual Clauses, incorporated into our DPA. For US data transfers, Barracuda is self-certified under the Data Privacy Framework. Find the certification here.

Location of Customer Data

ATP Service is hosted on the AWS cloud infrastructure. See the Security – Data Center Locations section below for more information.

Three types of data are collected by the Service: files, metadata about those files, and operational logs about the Service. All log data is stored in the US. No file content or personal data is included in the log data.

Data Retention

Files that Barracuda has (i) detonated (i.e.: opened) in the sandbox to watch and learn from the malicious behavior or (ii) deemed clean, are deleted immediately after scanning is complete and a log is generated. Virtual environments used for detonation are reset after each scan, eliminating any access to the file.

In cases where files are deemed malicious, Barracuda may maintain copies of those files in our Threat Data to further improve security and train machine learning systems. This Threat Data is considered Systems Data as defined in the Barracuda Legal Terms and Conditions.

This ensures that our customers benefit from the most up-to-date threat detection within the Products and Services that contain ATP.

Security

Data Transmission and Storage

Data Transmission

All communication between the ATP Service and the Barracuda Product or Service is SSL encrypted, including transport of the file itself. Any malicious files retained as Threat Data are stored in secure locations, accessible only by Barracuda's threat research team, partner organizations, and engineering staff with directly applicable job requirements to access these files. In every case, rigorous technical and security controls are in place to protect these files and systems. All computer systems exist in protected data centers that utilize both physical and electronic access controls; all access is monitored and audited.

Data Center Locations

The cloud infrastructure for ATP is deployed in the following geographical regions in accordance with customer preferences or product functionality.

AMERICAS:

- AWS Region - US East 1 – Virginia
- AWS Region – US East 2 - Ohio
- AWS Region - US West 1 – California
- AWS Region – US West 2 - Oregon
- AWS Region - Canada

EU:

- AWS Region – Germany
- AWS Region - Ireland

APAC:

- AWS Region - Japan
- AWS Region – Singapore
- AWS Region - India
- AWS Region – Australia

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.