Barracuda Managed Vulnerability Security 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 Managed Vulnerability Security 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. When MSPs provide their end customers with access to the Service, the MSPs pass through to their end customers 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.

OVERVIEW

The Service provides organizations with regular vulnerability scans that deliver comprehensive insights into your security landscape. Coupled with expert reporting, this service helps you understand your vulnerabilities in context, enabling you to prioritize remediation efforts effectively.

UNIT OF MEASURE AND LIMITATIONS

Subscriptions to this Service are sold on a *per-device basis*, encompassing any device on the Customer's network with an IP address. Examples include, but are not limited to desktops, laptops, servers, virtual infrastructure, etc. Each device scanned under this Service will be counted individually for usage metrics.

As further described below, installation and deployment of the Service is a shared responsibility between Barracuda and the Customer. Once the Service is installed and enabled Barracuda will provide:

- Comprehensive Setup: Initial configuration of the Service, including Device scanning.
- Scan Management: Efficient oversight and scheduling of vulnerability scans that periodically assess the network to identify certain risks.
- Vulnerability Assessment: In-depth scanning of all Devices to uncover potential security weaknesses.
- Reporting: Vulnerability reports delivered quarterly by default, with remediation guidance and practices for addressing identified vulnerabilities, provided in the Barracuda XDR Dashboard to support effective remediation efforts. The Service may accommodate monthly or every other month, upon request.
    - Ad Hoc Reporting: Customers may request 1 ad hoc scan / calendar quarter to accommodate auditing requirements.
- Dedicated Support Access: Support team available to address any inquiries related to the scanning process and vulnerability management.

Overage. If a customer uses the Service in excess of the number of Devices purchased, Barracuda may notify the customer so that the customer can purchase additional Device coverage or reduce the number of Devices to be consistent with the number already purchased. If the customer does not adjust the number of Devices within 30 days of the date of Barracuda's notice, ("Notice Period") then Barracuda may charge the customer at Barracuda's then-current list price for the Devices scanned in excess of the number the customer purchased.

MSPs. 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.

INSTALLING THE SERVICE

The Services are integrated into the end customer's environment as described below.

- ***Scoping*:** A Barracuda Solutions Architect will work with the Customer to gather the necessary information to properly establish the scope. The key information that needs to be defined at this stage is the expected volume of assets (any device/system with an IP address connected to the network), the number of sites and how they are connected, and the environment in which the scanning applications will be installed (Windows or Linux servers and physical servers, virtual servers, or cloud resources). Note that the Customer must own all assets that Barracuda will scan. Barracuda will not scan assets owned by a third party.

- ***Provisioning***: The Customer will provision the required dedicated servers to host the scanning applications. Note that the Customer is responsible for providing this infrastructure.
- ***Application installation***: Once the Customer provisions the dedicated servers, the Customer must download and install the scanning application. The Service uses third party scanning software, which Customers install on their devices to gather information used to create the security reports.
    - The first dedicated server will host the "Security Console" application.
    - The second dedicated server will host the "Scan Engine" application.
    - For organizations with multiple sites or larger volumes of assets, additional scan engine(s) may be needed.
- ***Connectivity***: The Customer will configure a NAT policy within their firewall or perimeter systems to allow connectivity between the Security Console and the Barracuda SOC secure network. This will enable the Barracuda SOC to manage the scanning.
- ***Configuration:*** Once the deployment described above is complete, the Barracuda SOC will work with the Customer to configure the scan. This includes but is not limited to defining target networks and any exclusions, setting a scan schedule based on the quarterly, monthly, or semi-monthly cadence, setting up authenticated scanning if applicable, and customizing scan templates if needed.

CUSTOMER RESPONSIBILITIES

Notwithstanding any other provision of the Agreement or Barracuda's assistance, Customers are responsible for the following:

- ***Defining scan targets***: The Customer is responsible for informing the Barracuda SOC of the networks they have within their environment which they wish to be scanned as part of this service.
- ***Reviewing scan reports***: It is crucial that the Customer review the reports that the Barracuda SOC provides upon completion of the scans. These reports outline the vulnerabilities identified and actions the Customer needs to take to resolve them.
- ***Patching:*** The Customer is responsible for patching/remediating the vulnerabilities identified by the scans.
- ***Network changes***: The Customer must notify the Barracuda SOC if they make any network changes that are relevant to vulnerability assessment. An example of this includes the organization provisioning a new subnet within their environment which needs to be included in the scan targets to be assessed.
- ***Maintenance and availability of host infrastructure***: The Customer is responsible for ensuring the dedicated servers hosting the scanning applications are running, healthy, and properly maintained. If any issues arise with connectivity or otherwise, the Customer is responsible for troubleshooting and resolving those.

- ***Protect end customer sensitive information*:** The Customer is accountable for implementing measures to avoid sending in security logs or communications related to the Service sensitive personal information, including without limitation, credit card numbers, social security numbers, national insurance numbers, tax filing number, Permanent Account Numbers, or any other numbers assigned to individuals.
- ***Customer-provided Third Party Software***: In situations where the 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 the end customer data and information about the end 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 end customer.

SERVICE LIMITATIONS

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.

Barracuda will perform only the Services set forth in the Order accepted by Barracuda. The warranties and limitations stated in the Agreement apply to the Services described in this Service Description.

Methodology Based Services. Services that Barracuda performs for its Customers follow a defined methodology, rather than being driven by a specific end result or deliverable. Accordingly, Barracuda cannot guarantee the outcome of its monitoring, testing, assessment, forensics, or remediation methods as all such methods have reliability limitations because the security threat landscape is extremely dynamic. Barracuda cannot guarantee that every system weakness, noncompliance issue, or vulnerability will be discovered during the performance of the Services. Barracuda uses industry accepted sampling methodology which attempts to reduce the cost to the Customer while minimizing the impact to the accuracy and reliability of the results. Customer acknowledges and accepts that limitations and inherent risks exist from approaches used by Barracuda to deliver the Services.

Indirect Connection Methods. The obligations of Barracuda to perform Services are dependent on Barracuda's ability to connect directly to the end customer devices on the end customer's network from Barracuda's SOC. If and to the extent that Barracuda is required to connect to end customer devices via the end customer's VPN or other non-

standard means, then to the extent that Barracuda is required to make adds, moves, or changes to or otherwise access such devices in connection with any incident response or help desk request, Barracuda will have no responsibility or liability for any failure to perform or delay in performing its obligations hereunder to the extent such failure or delay is caused by such indirect access.

Barracuda Access to End Customer Data. The Customer acknowledges that data, including names, email addresses, IP addresses, hostnames, geo locations, device names, and other information; contained within systems onboarded to the Services is accessible for Barracuda to monitor, analyze, and respond to security-related issues. Barracuda may download such data (e.g., as proof of access). The Customer is responsible for obtaining any necessary consents and warrants that it has secured all legally required permissions for Barracuda to deliver the Services.

No Legal Advice. Customer understands that, in connection with providing the Services, Barracuda may discuss topic that relate to legal issues. Barracuda does not provide legal advice or services, and none of the Services shall be deemed, construed as, or constitute legal advice. The Customer is ultimately responsible for retaining its own legal counsel to provide legal advice. Furthermore, any written summaries or reports provided by Barracuda in connection with any Services shall not be deemed to be legal opinions and may not and should not be relied upon as proof of or any guarantee or assurance as to Customer's legal or regulatory compliance, although Barracuda acknowledges that Customer has the right to rely on any written summaries or reports for the intended purposes of those summaries and reports.

Services are Point-in-Time Information. Customer understands that the Services do not constitute any guarantee or assurance that security of the end customer's systems, networks, and assets cannot be breached or are not at risk. These Services are an assessment, as of a particular point in time, of the performance of end customer's systems, networks and assets, and any compensating controls. Furthermore, Barracuda is not responsible for updating its reports and assessments or enquiring as to the occurrence or absence of such, considering subsequent changes to the end customer's systems, networks, and assets after the date of Barracuda's final report.

Limitation on Liability. **Notwithstanding any contrary terms between the end customer and MSP, MSP and Barracuda, or Customer and Barracuda, and unless prohibited by applicable law, Barracuda is not liable or responsible to Customer, MSP, end customer, or any third party claiming on behalf of an end customer or MSP for any amount of damages above the aggregate dollar amount paid to Barracuda for the purchase of the Services in the 6 months preceding the claim.**

No Indirect Damages. **Barracuda has no liability for lost profits (even if they arise from the events that generated the damages), loss of business, loss of data, loss of use of data, interruption of business, or for any indirect, special, incidental, consequential, or punitive damages, whether under the Agreement or otherwise, even if Barracuda has been advised of the possibility of such loss and notwithstanding the failure of the essential purpose of any limited remedy. Barracuda has no liability for representations or warranties provided by MSP or any other third party.**

DATA PROTECTION AND DATA SECURITY

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 GDPR 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.

Location of Customer Data. The Service stores customer data on Amazon Web Services (AWS) cloud infrastructure in the United States.

Access Control. Barracuda personnel may only access customer data at rest in certain circumstances including, for example, to provide support where access is necessary to address the customer's concerns and requests. Customers can manage who has administrative access to the Service account through the Barracuda XDR Dashboard.

***Data Retention During Subscription* Period**. The Service transmits the data from the vulnerability assessments conducted against the customer's environment to the Barracuda cloud tenant. Once received, the data is indexed and stored using AES 256-bit encryption in our secure AWS VPC environment.

Barracuda keeps reports in its cloud tenant for 90 days and then deletes them. Customers may export their reports so long as the reports remain in the Barracuda cloud tenant.

Data Center Security and Data Residency. The Service uses the AWS cloud infrastructure. The data center provider's compliance documentation is at: *AWS Trust Center: Customer Trust & Security - AWS Trust Center*.

The storage locations for data used for the Service are set forth below. Barracuda stores customer data at rest in in the same geographic region as the Customer. Once a customer selects a storage location, the customer data will not be stored or failed over outside the region in which the customer selected.

- AWS Region - US East - 1
- AWS Region - EU West -1
- AWS Region - EU Central - 1
- AWS Region - AP South - 1
- AWS Region - CA Central - 1

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.

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 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."

END OF SALE AND END OF SUPPORT

See the Barracuda End of Sale and End of Support Policy on the Trust Center. 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.