Schedule A

Data Processing Profile

Radware’s Bot Manager Service

This Data Processing Profile is supplemental to a Data Processing Agreement (“**DPA**”) between Radware Ltd./Inc. (“**Radware**” or “**Processor**”) and the entity that has executed or accepted the DPA (“**Customer**” or “**Controller**”). This Data Processing Profile describes the processing of personal data (or personal identifiable information) by Radware in connection with Radware’s **Bot Manager Service** (the “**Service**”). Capitalized terms used in this Data Processing Profile but not defined herein shall have the meanings ascribed to them in the DPA.

Service Overview

Supplier’s Bot Manager Service provides protection to web applications, mobile apps and APIs from automated attacks using bots. The Service makes precise decisions to distinguish between activity of human visitors, activity of legitimate automated software systems (i.e., good bots) and activity of malicious automated software systems (i.e., bad bots) so that mitigation controls can be put in place to limit automated and programmatic web and mobile application malicious access. The Service uses several proprietary techniques, a combination of deterministic and machine learning models, to distinguish and detect automated software systems, including but not limited to intent based deep user behavioral analysis that gather signals across user requests to detect and block malicious bots.

The Service provides the flexibility to configure various bot mitigation options based on the bot generation, bot category, specific page URL and geography. The Service also provides granular analytics and reporting functionality for customers through the Radware Unified Cloud Service Portal (“Service Portal”).

The Service may be deployed either through a customer on-prem integrated agent, virtual appliance or a DNS diversion mode using Radware Cloud Application Protection package offerings.

Purpose of the Processing

Processing is performed to protect the assets of the Customer that are covered by the Service (the “Protected Assets”) from automated threats caused by malicious actors; all pursuant to and for the limited purpose of performing Radware’s obligations set out in the Principal Agreement (as defined in the DPA).

Processing of Data in Transit

The Service processes traffic (legitimate and malicious) targeted at the Protected Assets through a Radware Bot Manger POP (Radware has about 21 POPs in Google Cloud Platform (GCP) to receive traffic from Radware’s customers). This is setup in such a way that traffic from the customer’s integration point will reach the nearest

POP. From the POP, the traffic is sent for more detailed analysis to the Bot Manager backend through a secure channel. We also have a PoP in Amazon Web Services, (af-south-1) to process traffic.

The Service collects HTTP headers and browser information (through JavaScript) to fingerprint the source of the end user device and leverage this information for accurate bot detection process. In terms of the personal data, Radware Bot Manager only collects the IP Address from the HTTP Header received from an HTTP request of an end user and User ID (a **non-mandatory** parameter collected only if the Customer wishes to share this information with Radware). This User ID value is hashed in the API call made to the Radware Bot Manager engine. Additionally, with respect to ‘privacy by design’, Radware offers a feature in NginX connector / agent to selectively collect/discard the headers if the Customer believes that the information can potentially be a Personally Identifiable Information.

Data in transit at network level & application level is encrypted using TLS 1.2 (AES 128).

Processing of Data at Rest

The Service does not store any information that can directly identify a natural person.
The Service only stores information on malicious actor activity (including malicious source IP addresses and malicious headers), alongside aggregated non-identifiable statistics about legitimate users.
Data at rest includes encryption at hardware / storage level using AES 256 / AES 128.

Radware’s cloud partner (Google Cloud Platform (GCP)) uses advanced encryption mechanism – Cloud Key Management System Customer-Managed Encryption Keys (CMEK) on Google Kubernetes Engine (GKE) using Cloud Key Management System.

A very limited scope of Personal Data is required for Radware to perform its support services. In this respect, Information transferred to the U.S., India, and Columbia, is limited to log entries and network traffic directly related to problem resolution or attack mitigation. In addition, contact information for the customer’s support team responsible for interacting with Radware may be accessed from each site.

Items of Data stored by the Service

Repository	Data Description	Retention Period
Customer Portal Database	Security Event Metadata for the purpose of presenting status and statistics to the Customer through	For Security Event Metadata, the maximum retention period is 7 days.

	the Service Portal and managing the Service. The metadata includes: Attacker/malicious actor information: - Source IP - Source country - User-agent - Session cookie data Attack/malicious activity information: - Bad Bot Category - Violation Details - Policy ID - Attacked URL - Bot Signature and its Expiry Time Request headers - Accept Header - Referrer Bot Analytics data presented on the Unified Cloud Services Portal for customers to have a deeper analysis of the bad bot, legitimate bot and Crawler data accessing their applications. In this, the following data is presented on the Unified Cloud Services Portal: 1. IP address 2. ISP 3. City and Country	Data Deletion: data is deleted at the end of the applicable retention period set forth above. Radware Bot Manager provides facility for the Customer to request to delete the data of selective or collective data subjects directly from the Service Portal.

	4. Bot Category/Security Module 5. Number of hits from that source 6. Action taken by Bot Manager 7. Bot Characteristics 8. Top URLs accessed 9. Top Referrers 10. Top User Agents 11. Top Sections For Legitimate and Crawler data, the following data is presented 1. Crawler/Legitimate Bot Family Name 2. Legitimate Bot Category Name (for legitimate bots) 3. Total Hits 4. Top IPs	
Bad Bot Analyzer Security Analysis Services	Server log file: Applicable only in cases where the Customer requests a bad bot analyzer report. The bad bot analyzer is a free service offered by Radware that can be leveraged by the Customer either during a sales or presales phase to understand the volume and impact of bots to its business by scanning the data available in the log. The Customer will be able to send its server logs through a secure encrypted channel.	For Bad bot Analyzer request: The server log retention period is 7 days.
Bot Manager Data Warehouse for processing and	Radware Bot Manager uses Google Cloud BigQuery (BQ) as a data warehouse for processing and analyzing customer data. BigQuery is	30 days of data is stored in Google BigQuery.

analyzing Customer data	hosted on Google Cloud and provides scalable, secure, and high-performance analytics capabilities. Data stored in BigQuery is encrypted at rest and in transit, adhering to Google Cloud's security and compliance frameworks.	
Account Information	Data related to the account protected by the service. Subscription: - Account name - Subscription period - Service plan - Contact information - Portal users details	Stored as long as the Customer account is active. Deleted once Customer stops using the Service.
Audit Logs	Records different actions taking place in the Service: User Activity: - Login - Logout - User creation, modification, and deletion Configuration Changes: - Asset activation - Asset configuration changes Account Configuration Changes: - Account provisioning and deletion - Account settings modifications	2 years (3 months available for review through the Service Portal)

The above data is stored in virtual private cloud (VPC) environments based in the United States **or** Europe (GCP) depending on the Customer's choice. Radware has stringent access control for the data set of the Customer's application. This data is only accessed by the Customer (and whomever the Customer gives permission to, e.g., a service provider), privileged users (for example, security analysis team member in case of any issues reported/proactive analysis) and by the Radware ERT team (for the purpose of providing the managed Service). The Customer may receive alerts of blocked bot attacks or view status via the online Service Portal.

Data Subjects

Individuals about whom data is provided to Radware through or in connection with the Service by (or at the direction of) the Customer or by the Customer's end-users, which may include any natural person who accesses the Customer's Protected Assets as well as employees, agents or advisors of the Customer.

Duration of the Processing

The duration of the processing is determined by the Principal Agreement (as defined in the DPA) or until the deletion of all of Customer's Personal Data in accordance with the DPA and the "Data Retention and Deletion" details set forth in the table above.

Processing Locations

Approved Sub-Processor/Affiliate (Company Name)	Company Address	Approved scope of work	Approved Service Locations	Service Location address
Google	Mountain View, California	PoP	us-east1	Moncks Corner, South Carolina, USA
Google	Mountain View, California	PoP	us-east4	Ashburn, Northern Virginia, USA
Google	Mountain View, California	PoP	us-west1	The Dalles, Oregon, USA
Google	Mountain View, California	PoP	us-west2	Los Angeles, California, USA
Google	Mountain View, California	PoP	us-west3	Salt Lake City, Utah, USA

Google	Mountain View, California	PoP	us-west4	Las Vegas, Nevada, USA
Google	Mountain View, California	PoP	us-central1	Council Bluffs, Iowa, USA
Google	Mountain View, California	PoP	europe-west1	St. Ghislain, Belgium, Europe
Google	Mountain View, California	PoP	europe-west2	London, United Kingdom
Google	Mountain View, California	PoP	europe-west3	Frankfurt, Germany
Google	Mountain View, California	PoP	europe-west4	Eemshaven, Netherlands
Google	Mountain View, California	PoP	europe-north1	Hamina, Finland
Google	Mountain View, California	PoP	asia-east1	Changhua County, Taiwan
Google	Mountain View, California	PoP	asia-southeast1	Jurong West, Singapore
Google	Mountain View, California	PoP	asia-south1	Mumbai, India
Google	Mountain View, California	PoP	australia-southeast1	Sydney, Australia
Google	Mountain View, California	PoP	asia-east2	Hong Kong
Google	Mountain View, California	PoP	asia-northeast1	Tokyo, Japan
Google	Mountain View, California	PoP	asia-northeast3	Seoul, South Korea
Google	Mountain View, California	PoP	northamerica-northeast1	Montréal, Québec, Canada
Google	Mountain View, California	PoP	southamerica-east1	Osasco, São Paulo, Brazil, South America

Google	Mountain View, California	Backend engine	europe-west3	Frankfurt, Germany
Google	Mountain View, California	Backend engine	us-central1	Council Bluffs, Iowa, USA

Amazon	Seattle, Washington	PoP	af-south-1	Cape Town, South Africa

Technical and Emergency Support

Technical and Emergency Support is provided to Radware customers according to the agreed Service Level Agreement (SLA). The support services may be provided by ERT Analysts based in Chennai India, Tel Aviv Israel, New Jersey USA, and Bogota Columbia.

Industry Standard Certificates

Being Part of the Radware Cloud Services Offering, Radware Bot Manager Service complies with the following standards for cybersecurity and privacy:

-
- *ISO 22301* Business Continuity Management System
- *ISO 27001* *Information Security Management System*
- *ISO 27032* *Security Techniques -- Guidelines for Cybersecurity*
- *ISO 27017* *Information Security for Cloud Services*
- *ISO 27018* *Information Security Protection of Personally identifiable information (PII) in public clouds*
- *ISO 27701* *Data Privacy Management System*
- *HIPAA* *Health Insurance Portability and Accountability Act*
- *PCI-DSS* *Payment Card Industry Data Security Standard – Service Provider Schedule D*

Radware is compliant with *ISO 28000 Specification for Security Management Systems for the Supply Chain.*

Radware maintains a current SOC2 type II report for the Cloud Bot Manager Service

Compliance with these standards is audited annually by third party auditors.

Customer may find Radware’s latest cybersecurity and privacy certifications and attestations in https://www.radware.com/newsroom/certificationsindustry/.

North America

Radware Inc.

575 Corporate Drive

Mahwah, NJ 07430

Tel: +1-888-234-5763

International

Radware Ltd.

22 Raoul Wallenberg St.

Tel Aviv 6971917, Israel

Tel: 972 3 766 8666