Schedule A

Data Processing Profile

Radware's Cloud DDoS Protection 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 personally identifiable information) by Radware in connection with Radware's **Cloud DDoS Protection 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

The Service is a cloud-based service designed to protect data centers, networks and servers of the Customer (the "**Protected Assets**") against Distributed Denial of Service (DDoS) attacks, by providing multi-vector DDoS attack detection and mitigation.

The Service is powered by a global cloud security network with dedicated scrubbing centers spread globally (each, a "**Radware Scrubbing Center**"). Traffic directed at the Customer's Protected Assets, is being redirected to a Radware Scrubbing Center. In the Radware Scrubbing Center, the Customer's traffic is inspected for attempts to flood the network or overwhelm specific application resources, and cleaned of malicious DDoS attack traffic, where the remaining clean (legitimate) traffic is forwarded to the Customer's Protected Assets. Application payload data is not processed or stored by the Processor.

The Service features a Service Portal which provides visibility and self-service management of the Service elements through the Radware Unified Cloud Service Portal ("Service Portal").

<u>AI SOC Xpert</u>

The Customer may activate an optional SOC Xpert module. AI SOC Xpert enhances the Customer's security operations by providing real-time attack context, wave-based insights, and AI-driven mitigation recommendations. The solution offers improved visibility across evolving DDoS attack patterns and supports faster, more informed decision-making during active events.

By streamlining investigation workflows and reducing manual analysis, AI SOC Xpert helps security teams validate and optimize mitigation actions with greater accuracy. This results in faster response, reduced operational effort, and strengthened overall defense posture during complex DDoS incidents.

AI SOC Xpert processes attack-related telemetry and operational event data solely for generating insights and recommendations for the specific Protected Assets. Such data is retained for up to three months and is then automatically deleted.

Purpose of the Processing

Processing is performed to protect the Customer's Protected Assets from distributed denial of service (DDoS) attacks; 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

Cloud DDoS Data Flow – Always-on and Hybrid Always-on:

Traffic (legitimate and malicious) from users of the Protected Assets normally transits through a Radware Scrubbing Center that is in the same region as the Protected Assets. Attack traffic is scrubbed at the local Radware Scrubbing Center and possibly at another Radware Scrubbing Center closer to the attack source in case of a large DDoS attack, traffic load balancing or a Service failure (redundancy). Data in transit may include all categories of Personal Data.

Cloud DDoS Data Flow – On-demand and Hybrid On-demand:

Traffic (legitimate and malicious) from users of the Protected Assets normally transits to a data center owned by or operated on behalf of the Customer and hosting the Protected Assets. In case of a DDoS attack, the traffic is diverted to a Radware Scrubbing Center that is in the same region as the Protected Assets. Attack traffic is scrubbed at the local Radware Scrubbing Center and possibly at another Radware Scrubbing Center closer to the attack source in case of a large DDoS attack, traffic load balancing or a Service failure (redundancy). Data in transit may include all categories of Personal Data.

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 in some cases source IP addresses), alongside aggregated non-identifiable statistics about legitimate users. Furthermore, the Service allows encryption of source IP addresses values prior storage.

Items of Data at Rest stored by the Service

Category	Data Description	Retention Period
Protected Assets Data	Security event metadata for the purpose of presenting status and statistics to the Customer through the Service portal, generating reports and managing the Service. The metadata includes: - Malicious source IP addresses - Traffic statistics (BPS, PPS) - Attack statistics (vector, sources, destinations) - Attack type	Deleted using cryptographic erasure after 180 days
Account Information	Data related to the account protected by the Service: - Account name - Service plan - Contact information - Portal Users - Protected Assets information	Stored as long as the account is active.
Audit Log	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 Service Portal)

The above data is stored in virtual private cloud (VPC) environments based in the Google Cloud Platform (GCP) in Frankfurt, Germany. This data is only accessed by the Customer (and whomever the Customer gives permission to, e.g., a service provider) and by Radware for the purpose of providing the Service.

The Customer may receive alerts of blocked attacks or view status via the online Service portal.

The Cloud DDoS Protection Service Portal, Security Log and configuration database are stored within the EU.

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.

Data Subjects

Individuals about whom data is provided to Processor through or in connection with the Service by (or at the direction of) the Customer or by the Customer's end-users, that 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 or until deletion of all Customer's data in accordance with the DPA and the "Retention Period" set forth in the table above.

Processing Locations

Approved Sub-Processor/Affiliate (Company Name)	Company address	Approved scope of work	Approved Service Locations	Approved Service Locations - Address
Radware	Raoul Wallenberg Street 22, Tel Aviv-Yafo, Israel	DDOS Scrubbing Center	Frankfurt (FRA)	Company: Digital Realty Address: Weissmüllerstrasse 264, Frankfurt am Main, 60314, Germany
			London (LON)	Company: Equinix - LD7 Address: 1 Banbury Ave, Slough, London,

				SL1 4LH, United Kingdom
			Ashburn (ASH)	Company: Equinix - DC2 Address: 21715 Filigree Court, Ashburn, Virginia 20147, US
			Dallas (DAL)	Company: Equinix - DA3 Address: 1950 N Stemmons FwySuite 1039A, Dallas, Texas, 75207, US
			San Jose (SJC)	Company: Equinix - SV11 Address: 5 Great Oaks Blvd, San Jose, California, 95119, US
			Tokyo (TKO)	Company: Equinix -TY2 Address: 3 Chome-8-21 Higashishinagawa, Shinagawa City, Tokyo 140-0002, Japan
			Hong Kong (HKG)	Company: Equinix - HK1 Address: Unit 2702, 27/F, Goodman Global Gateway, 168 Yeung Uk Road, Tsuen Wan, Hong Kong
			Sydney (SYD)	Company: Equinix - SY2 Address: 639 Gardeners Road Unit B, Mascot 2020, Sydney, New South Wales, Australia
			Seoul (SEO)	Company: KINX Address: 5F, Daelim Acrotel, 13, Eonju-ro

				30-gil, Gangnam-gu, Seoul, South Korea
			Johannesburg (JNB)	Company: Teraco - JB1 Campus buildings DC6/DC10 Address: 5 Brewery Street, Isando, Johannesburg, Gauteng, South Africa
			Tel Aviv (TLV)	Binat Raoul Wallenberg 24 Tel Aviv. Israel
			Sao Paulo (GRU)	Company: Equinix - SP3 Address: Av. Marcos Penteado de Ulhôa Rodrigues, 249 - Res. Tres (Tambore), Santana de Parnaíba - Sao Paulo, CEP: 06543-001, Brazil
			Chennai (MAA)	Company: Nxtra Data Limited- Chennai-DC 1 Address: F-8 SIPCOT–IT park, Siruseri, Chennai Tamil Nadu 603103, India
			Amsterdam (AMS)	Company: Equinix - AM3 Address: Science Park 610, XH Amsterdam, 1098, Netherlands
			Taiwan (TPE)	Company: Chief Telecom Inc Address: No. 37, H.D building, Lane 188, Ruiguang Rd, Nei-hu Dist., Taipei 114, Taiwan
			Dubai (DXB)	Company: Equinix - DX1

				Address: Units F88 – F92, Dubai Production City Sheikh Mohammed Bin Zayed Rd Dubai, UAE 500389, United Arab Emirates
			Toronto (YYZ)	Company: Digital Realty - YYZ12 Address: Suite 207, 151 Front St W, Toronto, ON M5J 2N1, Canada
			Melbourne (MEL)	Company: Digital Realty - MEL11 Address: 72 Radnor Drive, Deer Park, Melbourne, 3023, VIC, Australia
			New Zealand (AKL)	Company: Spark Digital Address: Spark Building, Datahall 2, Level 5, 31 Airedale St, 1010, Auckland, New Zealand
			Paris (CDG)	Company: Digital Relaity PAR8 Address: 2 Avenue Marcel Cachin, 93120 La Courneuve, France
			Mumbai (BOM)	Company: C/O Yotta Data Services Private Limited - NM1 DC Address: 1ST, 2ND & 3RD LEVEL EDINBERG BUILDING,SURVERY NO 30. BHOKAR PADA VILLAGE,PANVEL RAIGAD - 410 206.Mumbai, India

Google Cloud - GCP		Operate Cloud Service Portal	Europe – West3	Frankfurt am Main, Germany
			Bogota (BOG)	Company: Equinix Colombia Inc Nit 900.195.141-1 Carrera 106 15A-25 Manzana 18 Lotes 125, 126 Y 127 Zona Franca Bogota Bogota 110921, Colombia
			Lima (LIM)	Company: Cirion - LIM1 Address: Avenida Manuel Olguín 395, Santiago de Surco – Lima
			Singapore (SIN)	Company: Equinix SG3 Address: 26A Ayer Rajah Crescent, Private Lot FX1-4a, Singapore, 139963 Singapore
			Rosh Ha'ayin (TLV05)	Company: Partner Address: Hamelaca 16 Rosh Ha'ayin 48, Israel

Industry Standard Certificates

Radware complies with the following standards for cybersecurity and privacy:

- ISO 22301 Business Continuity Management System
- *ISO 27001 Information Security Management Systems*
- *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*
- *ISO 42001- Artificial Intelligence Management System*
- *HIPAA Health Insurance Portability and Accountability Act*

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 DDoS 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

© 2026 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.