

Schedule A

Data Processing Profile

Radware's Cloud Web Application Firewall (CWAF) 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 Web Application Firewall (CWAF) 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

Radware's Cloud Web Application Firewall (CWAF) Service protects web applications and application programming interfaces (“APIs”) (the “Protected Assets”) against Web application layer attacks.

The Service is provided through a global network of distributed Points of Presence (“PoPs”), using an optimized and highly available architecture. This architecture enhances the Service’s performance and availability.

The Service’s PoPs are located at major traffic hubs with connections to tier-1 ISPs, striving for low latency and minimal impact on Protected Asset’s performance.

The Service features a Customer Service Portal, which provides visibility into the alerts and function of the Service. Configuration options, such as uploading SSL certificates, signature files and application definitions may be defined and managed using the Service Portal.

The Customer may activate an optional API Discovery feature. The API Discovery Feature conducts additional evaluation of the network traffic flow, searching for applications that are not currently protected by the Service. During the API Discovery process, 24 hours’ worth of network traffic is collected and then analyzed, offline, for an additional 48 hours. At the conclusion of the analysis phase, recommendations are sent to the Customer and the collected information is deleted. This information is processed and stored within the region it was collected from.

Purpose of the Processing

Processing is performed to protect the Customer’s Protected Assets from web application attacks, such as the “OWASP Top 10 Web Attacks”.

Processing of Data in Transit

The Service processes all network traffic (legitimate and malicious) flowing to the Protected Assets through a Radware PoP located in the same region. Additional PoP(s) may be selected within the same



region to support load balancing and to provide redundancy. In the case of a large DDoS attack, traffic may be processed at a Radware scrubbing center(s) closer to the source of the attack. These additional locations are listed below.

Data in transit may include all categories of Personal Data as is transmitted in the Customer’s data stream. Processing activity includes traffic decryption, security inspection and re-encryption of the traffic and then forwarding to the Customer’s Protected Assets.

To permit the inspection of the SSL traffic, the Service requires the Customer to securely upload its SSL keys onto the Service Portal using secure storage. The Service, using an automated process, loads the keys into the appropriate infrastructure devices.

Processing of Data at Rest

The data residing on the Customer Service Portal includes metadata on malicious activity (including malicious source IP addresses and network headers): Customer’s account and configuration information: Audit Logs (i.e. Customer’s interaction with the Services Portal) and aggregated statistics about legitimate traffic. Such data contains limited personal data, mainly in the form of IP addresses and fragments of transaction data. The Service Portal encrypts the malicious source IP values prior to storage.

Access to the Customer Service portal requires the use of Multi-Factor Authentication and the HTTPS protocol.

The Customer Service Portal database is currently hosted, using AWS Cloud Services, in the US. By the end of the first quarter of 2022, the database will be hosted within the EU. The Service Portal visualization layer processing will be performed in the U.S location with no data being stored.

Data stored by the Service

Repository	Data Description	Retention Period
Customer Portal Database	<p>Security event metadata for the purpose of presenting status and statistics to the Customer through the Service portal, generating reports and managing the Service.</p> <p>The following security alerts information is stored:</p> <p>Attacker/malicious actor information:</p> <ul style="list-style-type: none">- Source IP- Source country- User-agent	3 months

	<ul style="list-style-type: none"> - Session and cookie data <p>Attack/malicious activity information:</p> <ul style="list-style-type: none"> - OWASP category - Attack category - Attacked URL - Request headers - Response headers - Attack payload - Action taken 	
<p>Database POP</p>	<p>Security event metadata per pop for the purpose of presenting status and statistics to the Customer through the Service portal, generating reports and managing the Service.</p> <p>The following security alerts information is stored:</p> <p>Attacker/malicious actor information:</p> <ul style="list-style-type: none"> - Source IP - Source country - User-agent - Session and cookie data <p>Attack/malicious activity information:</p> <ul style="list-style-type: none"> - OWASP category - Attack category - Attacked URL - Request headers - Response headers - Attack payload - Action taken 	<p>1 week</p>
<p>Audit Log</p>	<p>The following operations are stored as part of the Audit Log (resulting from user action or API invocation).</p> <p>User Activity:</p> <ul style="list-style-type: none"> - Login - Logout - Failed login attempts - User creation, modification, and deletion <p>Application Configuration Changes:</p> <ul style="list-style-type: none"> - Application provisioning and deletion - Network configuration changes 	<p>2 years</p> <p>(3 months available for review through Service Portal)</p>

	<ul style="list-style-type: none"> - Security policy modification Account Configuration Changes: <ul style="list-style-type: none"> - Account provisioning and deletion - Account settings modifications 	
Account Information and configuration data	Data related to the Customer’s account in the Service Portal. Subscription: <ul style="list-style-type: none"> - Account name - Subscription period - Service plan - Contact information - Users 	Stored as long as the Customer account is active. Deleted once Customer stops using the service.
Regional Database Used to support the API Discovery Feature	User Transaction metadata for special features of the Service The following HTTP information is processed and stored: <ul style="list-style-type: none"> - Path - Method - Headers - Response code - Body 	48 hours

Data Subjects

Natural Persons include the users of the Customer’s Protected Assets and the Customer’s employees or agents who administrate the Service.

Duration of the Processing

The duration of the processing is determined by the Principal Agreement or until deletion of all Customer’s Personal Data in accordance with the DPA and the “Retention Period” set forth in the table above.

Processing Locations (PoPs)

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	Cloud WAF POP	Frankfurt (FRA)	Weissmuellerstr. 13, 60314 Frankfurt, Germany
			London (LON)	1 Banbury Avenue Slough SL1 4LH, Slough, GB, SL1 4LH
			Ashburn (ASH)	21715 Filigree Ct, Ashburn, VA 20147, USA
			Singapore (SIN)	IBM-SL / Digital Reality - 29A International Business Park, Jurong East, Singapore 609934
			San Jose (SJC)	IBM San Jose
			Tokyo (TKO)	12B, 3-4-1 Inukura, Miyamae-ku, Kawasaki-shi, Kanagawa 216-0011 - Japan
			Hong Kong (HKG)	ROYALE INTERNATIONAL COURIERS LTD, 585-609 CASTLE PEAK ROAD 3RD FLOOR GOODMAN KWAI CHUNG LOGIST HK
			Sydney (SYD-SL)	273 Pymont St Ultimo, Sydney NSW 2007, Australia
			Sydney (SYD2)	C/639 Gardeners Rd, Mascot NSW 2020, Australia
			Johannesburg (JNB)	5 Brewery Street, Isando, Johannesburg, South Africa

			Tel Aviv (TLV)	Ha-Sivim St 49, Petah Tikva, Israel
			Chennai (MAA)	IBM Chennai
			Sao Paolo (SAO)	IBM Sao Paolo
			Chicago (ORD)	2200 Busse Rd, Elk Grove Village, IL 60007, USA
			Moscow (MOW)	Butlerova str. 7, Moscow, Russia, 117485
			Amsterdam (AMS)	Amsterdam Science Park, Science Park 610, Amsterdam, 1098 XH, Netherlands
			Seoul (SEO)	IBM Seoul
			Toronto (YYZ)	45 Parliament St, Toronto, ON M5A 2Y5, Canada
Amazon Web Services (AWS)		Operate Cloud Portal (Presentation layer) Service Portal DB stores in Frankfurt (*)	US– East	VA, USA
			Frankfurt (FRA)	Weissmuellerstr. 13, 60314 Frankfurt, Germany
Microsoft Azure (Currently decommissioned)		Network Points of Presence (PoPs)	US East	VA, USA
			US North Central	IL, USA
			EU North	Dublin, Ireland
			EU France Central	Paris, France

(*) By the end of the first quarter of 2022, the database will be hosted within the EU.

Additional Processing Locations (scrubbing centers) that may be deployed during a severe DDOS attack

Approved Sub-Processor/Affiliate (Company Name)	Company address	Approved scope of work	Approved Service Locations	Approved Service Locations - Address
SecurityDAM	Raoul Wallenberg Street 24, Tel Aviv-Yafo, Israel	DDOS scrubbing center	Frankfurt (FRA)	Hanauer Landstraße 298, 60314 Frankfurt, Germany
			London (LON)	352 Buckingham Avenue, Slough, Berkshire, London, UK
			Ashburn (ASH)	21715 Filigree Court, Ashburn, VA, USA
			Dallas (DFW)	infomart, 1950 N Stemmons Fwy #1034, Dallas, TX, USA
			San Jose (SJC)	11 Great Oaks Blvd, San Jose, CA, USA
			Tokyo (TKO)	Financial Center North Tower 1-9-5 Otemachi, Chiyoda-ku, Tokyo, Japan
			Hong Kong (HKG)	399 Chai Wan Road, Hong Kong
			Sydney (SYD)	639 Gardeners Road Unit B, Mascot 2020, Sydney, Australia
			Seoul (KOR)	36, Jangmi-ro, Bundang-gu, Seongnam-si Gyeonggi-do KYUNG, South Korea
			Johannesburg (JNB)	5 Brewery Street, Isando, Johannesburg, South Africa

			Tel Aviv (TLV)	27 HaBarzel Street, Tel Aviv-Yafo, Israel
			Sao Paulo (GRU)	Av. Marcos Penteado de Ulhôa Rodrigues, 249 - Res. Tres (Tambore), Santana de Parnaíba, Sao Paulo, Brazil
			Chennai (MAA)	F-8 SIPCOT IT park, Siruseri, Navallur, Kancheepuram Distt, Chennai, 603103, India
			Amsterdam (AMS)	Science Park 610, 1098 XH Amsterdam, Netherlands

Industry Standard Certificates

Radware’s Cloud WAF Service complies with the following standards for cybersecurity and privacy:

- *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*
- *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 WAF Service

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

Customers may find Radware’s latest cybersecurity and privacy certifications and attestations at <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

© 2022 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.