

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 functions of the Service. Configuration options, such as uploading SSL certificates, signature files and application definitions may be defined and managed using the Radware Unified Cloud Service Portal (“**Service Portal**”).

Customer Selectable Features

Security Event Log Export

The Customer may activate an optional Security Event Log export. This feature allows customers to export all security events directly from the Cloud Application Protection Service to an AWS S3 bucket, Azure or SFTP. All security events from WAF, DDoS, and BOT are consolidated in a JSON format and automatically uploaded to a designated S3 bucket. This functionality empowers customers to seamlessly manage and analyze security events, providing a valuable resource for enhancing overall security strategy.

Access Log Export

The Customer may activate an optional Access Log Export. Enabling this functionality allows a customer to track the traffic to the application and troubleshoot issues with the server or website.

All transactions are streamed in a JSON format to the configured customer S3 bucket, SFTP or Azure Blob and detailed data regarding client access to the protected applications is provided.

During the activation process the access logs are data in transit and the maximum data may be retained by the service up to 48 hours.

Access Log Visibility

The Customer may activate an optional visualization of the access-log. Enabling this functionality allows a customer to track the traffic to specific applications and troubleshoot traffic issues.

Access-log Visibility is not available by default for all applications. It requires an Add-on to activate this feature on specific applications.

The activation of this feature will store the data per region for a maximum retention period of 48 hours.

Client-Side Protection

The customer may activate optional Client-Side Protection. With Client-Side Protection enabled, Cloud WAAP customers ensures the protection of end users' data from theft via client-side attacks such as formjacking, Magecart, supply chain, e-skimming and DOM based XSS.

It provides visibility and control over the JS services embedded in the application, can learn its risk and trace its sources.

Malicious JS activities are detected and reported in real-time and attempts to send data outside of the browser or interact with sensitive information are monitored, classified and assessed to give an accurate and intuitive threat level.

With Client-Side protection, source IP addresses may be stored in the Frankfurt, Germany backend for up to 24 hours.

Messages containing PII are sent to our backend using a proxy on the main domain. The PII is anonymized using European Data Protection Board (EDPB) recommended processes before it is stored.

Web DDoS protection

The Customer may activate an optional Web DDoS Protection. The Cloud Web DDoS Protection solution is specifically designed to address the growing threat of Web DDoS Tsunami attacks that can easily evade standard security measures. Our solution sets a new standard in combating encrypted, high-volume, multi-vector attacks, outperforming traditional web application firewalls (WAF) and network-based DDoS tools.

With its exceptional ability to learn application behavior and adapt to changing attack rates, our solution ensures optimal mitigation and protection. It minimizes false positives, offers comprehensive coverage against advanced threats including zero-day attacks, and provides an immediate and adaptive defense. Users can have peace of mind with our automated and fully managed system.

The Cloud Web DDoS Protection is ready to handle emergency situations by operating seamlessly, even without a learning period or prior knowledge about the application. It possesses the capability to dynamically generate customized signatures based on the characteristics of the attack HTTP request. This innovative approach enhances security by providing an additional layer of defense, ensuring swift and effective protection.

During the activation of Web DDoS Protection, transactions are processed and stored for three weeks in EU.

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 Cloud WAF Security Log and configuration database is stored within the EU.

Requests to view this log information are encrypted and routed through the Service Portal located in the US. No customer information is stored in the portal.

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 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 - 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>3 months</p> |

| | | |
|---|---|---|
| Database POP | <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> |
| Audit Log | <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 - Security policy modification <p>Account Configuration Changes:</p> <ul style="list-style-type: none"> - Account provisioning and deletion - Account settings modifications | <p>2 years</p> <p>(3 months available for review through Service Portal)</p> |
| Account Information and configuration data | <p>Data related to the Customer’s account in the Service Portal.</p> <p>Subscription:</p> <ul style="list-style-type: none"> - Account name - Subscription period - Service plan - Contact information - Users | <p>Stored as long as the Customer account is active. Deleted once Customer stops using the service.</p> |
| Security Events Export Feature | <p>Security event metadata per PoP /data base in EU for the purpose of export the security events</p> <p>The following security alerts information is stored:</p> | <p>Data Not Retained</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 | |
| Client-Side Protection Feature | <p>User transaction metadata for special features of the service</p> <p>The following HTTP information is processed and stored:</p> <ul style="list-style-type: none"> - Path* - Source IP <p>* PII anonymized before it is stored in the EU backend.</p> | <p>Path – No limit</p> <p>Source IP – 24 hours</p> |
| Web DDoS Feature | <p>User transaction metadata for special features of the service in EU</p> <p>The following HTTP information is processed and stored:</p> <ul style="list-style-type: none"> - Path - Method - Headers - Response code - Cookie - Source IP - Request size - Response size | <p>3 Weeks</p> |
| Access log Visibility | <p>User transaction metadata for special features of the service</p> <p>The following HTTP information is processed and stored:</p> <ul style="list-style-type: none"> • Path • Method • Headers • Response code • Source IP • Cookie • Request size • URI <p>Response size</p> | <p>48 hours</p> |
| | | |

Data Subjects

Natural Persons include the users of the Customer’s Protected Assets and the Customer’s employees or agents who administer 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) | Company: Digital Realty / Interxion Deutschland GmbH Address: Weissmüllerstrasse 34, Frankfurt am Main, 60314, Germany |
| | | | London (LON) | Company: Equinix - LD7 Address: 1 Banbury Ave, Slough, London, SL1 4LH, United Kingdom |
| | | | Ashburn (IAD) | Company: Equinix - DC3 Address: 44470 Chilum Pl., Building 1, Ashburn, VA 20147, US |
| | | | Singapore (SIN) | Company: Softlayer Technologies - SNG01 Address: 29A International Business Park, Jurong East, 609934, Singapore |
| | | | San Jose (SJC) | Company: Softlayer Technologies - SJC04 Address: 2001 Fortune Drive, San Jose, 95131, California, US |



| | | | |
|--|--|--|---|
| | | | <p>Tokyo (TYO)</p> <p>Company: Softlayer Technologies - TOK05</p> <p>Address: NTT - 3-4-1 Inukura, Miyamae-ku, Kawasaki City, Kanagawa Prefecture, 216-0011, Japan</p> |
| | | | <p>Hong Kong (HKG)</p> <p>Company: Equinix - HK1</p> <p>Address: Unit 2702, 27/F, Goodman Global Gateway, 168 Yeung Uk Road, Tsuen Wan, N.T., Hong Kong</p> |
| | | | <p>Sydney (SYD-SL)</p> <p>Company: SoftLayer Technologies Australia Pty Ltd/IBM Cloud</p> <p>Address: 273 Pyrmont Street, Ultimo, Sydney, NSW 2007, Australia</p> |
| | | | <p>Sydney (SYD2)</p> <p>Company: Equinix - SY2</p> <p>Address: 639 Gardeners Road Unit B, Mascot 2020, Sydney, New South Wales, Australia</p> |
| | | | <p>Johannesburg (JNB)</p> <p>Company: Teraco - JB1 Campus buildings DC6/DC10</p> <p>Address: 5 Brewery Street, Isando, Johannesburg, Gauteng, South Africa</p> |
| | | | <p>Tel Aviv (TLV)</p> <p>Company: Binat - Or towers building A Raoul Wallenberg 24 Tel Aviv, Israel</p> |
| | | | <p>Chennai (MAA)</p> <p>Company: Nextra Data Limited-Chennai-DC 1</p> <p>Address: F-8 SIPCOT-IT park, Siruseri, Chennai Tamil Nadu 603103, India</p> |

| | | | | |
|--|--|--|---------------------|--|
| | | | Sao Paolo (SAO) | <p>Company: IBM BRASIL-INDUSTRIAMAQUINAS E SERVICOS LIMITADA</p> <p>Address: Rua Presbitero Plinio Alves de Souza, 757 – J. Ermida II - Jundiai, SP 13212-181 – Brazil</p> |
| | | | Chicago (ORD) | <p>Company: Deft c/o DFT, Radware</p> <p>Address 2200 Busse Rd, Loading Dock, Elk Grove Village, IL 60007, US</p> |
| | | | Amsterdam (AMS) | <p>Company: Equinix - AM3</p> <p>Address: Science Park 610, XH Amsterdam, 1098, Netherlands</p> |
| | | | Mumbai (BOM) | <p>Company: C/O Yotta Data Services Private Limited - NM1 DC</p> <p>Address: 1ST, 2ND & 3RD LEVEL EDINBERG BUILDING,SURVERY NO 30. BHOKAR PADA VILLAGE,PANVEL RAIGAD - 410 206.Mumbai, India</p> |
| | | | AKL | <p>Company: Spark DigitalAddress: Spark Building, Datahall 2, Level 5, 31 Airedale St, 1010, Auckland, New Zealand</p> |
| | | | Toronto (YYZ) | <p>Company: Equinix - TR2</p> <p>Address: 45 Parliament Street, Toronto, Ontario M5A 0G7, Canada</p> |
| | | | Paris (CDG) | <p>Company: IBM France, S.A.S - PAR01</p> <p>Address: 7-9 rue Petit - 92582 Clichy – France</p> |
| | | | Petach Tikvah (PTK) | <p>Company: CCC</p> <p>Address: Hasivim 49, Petah Tikva, Israel</p> |

| | | | | |
|---------------------------|--|--|-----------------|--|
| | | | Chile (SCL) | Company: Claro Address: Liray 1120, Colina, Región Metropolitana, Chile |
| | | | Taipei (TPE) | Company: Chief Telecom Inc Address: No. 37, H.D building, Lane 188, Ruiguang Rd, Nei-hu Dist., Taipei 114, Taiwan |
| | | | Seoul (SEO) | Company: KINX Address: 5F, Daelim Acrotel, 13, Eonju-ro 30-gil, Gangnam-gu, Seoul, South Korea |
| | | | Dubai (DXB) | Company: Equinix - DX1 Address: Units F88 – F92, Dubai Production City Sheikh Mohammed Bin Zayed Rd Dubai, UAE 500389, United Arab Emirates |
| | | | Milano (MXP) | Company: IBM Italia c/o Campus DATA4 Address: Via Monzoro 103, Cornaredo, Milano 20007 |
| Amazon Web Services (AWS) | | Operate Cloud Portal (Presentation layer) Service Portal DB stores in Frankfurt | Frankfurt (FRA) | Weissmuellerstr. 13, 60314 Frankfurt, Germany |

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 |
|---|---|------------------------|----------------------------|---|
| Radware | Raoul Wallenberg Street 22, Tel Aviv-Yafo, Israel | DDOS Scrubbing Center | Frankfurt (FRA) | 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: Nextra 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 Relaiy 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 |

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

Radware’s Cloud WAF 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*
- *ISO 42001- Artificial Intelligence 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 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

© 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.