Cloud WAF
Service Agreement

October 2018

Contents

Cloud WAF Service Agreement

This Agreement, made this <Day> day of <Month>, <Year>, by and between RADWARE Ltd., having its principal place of business at 22 Raoul Wallenberg Street, Tel-Aviv, Israel 6971917, (hereinafter referred to as "Supplier"), and <Customer Name>, having its place of business at <Customer Address>, (hereinafter referred to as "Customer").

Supplier and Customer ("Parties") agree as follows:

1. Service Overview

The Supplier's Service includes several cloud-based modules providing protection from application-level attacks, network-level DDoS Attacks as well as Content Delivery Network (CDN) capabilities. A description of the features of each module is included in Appendix 2.

2. Service Levels

2.1. **Service Uptime Service Level**

All Service components will be available on a 99.999% basis ("**Service Uptime**").

2.2. **Time-To-Mitigation for DDoS Attacks**

As part of the Service, the Supplier commits to mitigating DDoS Attacks within the timeframes set forth in the table below for specific types of DDoS Attacks. The Time-To-Mitigation period will commence following successful detection of a DDoS Attack by the Supplier's Cloud Infrastructure and will end upon reaching Consistency-Of-Mitigation.

Time-To-Mitigation					
ICMP Floods	**UDP Floods**	**SYN Floods**	**TCP Flag Abuses**	***GET Floods**	***POST Floods**
5 min	5 min	5 min	5 min	15 min	15 min

**Relevant for both HTTP and HTTPS*

2.3. **Consistency-Of-Mitigation for DDoS Attacks**

The Supplier shall commit to providing a Consistency-Of-Mitigation level of no less than 95%. Consistency-Of-Mitigation is defined as being the proportion of the traffic that is forwarded to the Customer's Serviced Assets via the DDoS Protection module that is clean. The

Consistency-Of-Mitigation measurement window is defined as being the period following the Time-To-Mitigation and the End of Attack. If the Customer believes the Supplier is in breach of Consistency-Of-Mitigation commitments as defined in this Agreement, the Customer should provide to the Supplier a packet capture of at least one hour in duration that identifies total attack traffic volumes as a proportion of the total traffic volume received from the DDoS Protection module for the period identified as failing to meet the defined DDoS Protection Service Levels.

2.4. **General Service Level Provisions**

The following terms and conditions apply to all Service Levels described in this Section 2.

2.4.1. The Service Levels described in this Section only apply with regard to Serviced Assets that have been verified via a successful Service Validation Procedure.

2.4.2. Geographic coverage, communication methods and response times to Customer's approaches are outlined in Supplier's Certainty Support Guide.

2.4.3. None of the Service Levels described in this Section 2 above apply, when and for as long as a Special Unavailability is ongoing.

2.4.4. Except for the Service Uptime and any other Service Level warranties described in this Section 2 and in Appendix 2 for any particular Service: (i) the Service is provided "AS IS" and Customer's use of the Service is at Customer's sole risk; and (ii) THERE ARE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

3. In Excess of the Service Plan Policy

3.1. In the event that the Legitimate Traffic Level is In Excess of the Service Plan Policy (traffic burst) the Supplier will extra charge the customer based on overload pricing. In the event that the Legitimate Traffic Level is In Excess of the Service Plan Policy more than three (3) times during a period of 30 days, the Customer will either immediately pay the Supplier for the appropriate Service plan covering the actual Legitimate Traffic Level of Customer as set forth in the Supplier's then current price list for the remainder of the then-applicable Service term, or immediately reduce its Legitimate Traffic Level to be within the Service plan purchased by the Customer. If the Customer does not act on any one of the above options, the Supplier shall be entitled to terminate the Service without the Customer being entitled to any remedies, refund, or any other form of compensation. A termination of the Service by Supplier as above, shall not absolve the Customer of its payment obligation for the entire Service term.

3.2. In the event that as a result of a DDoS Attack, the total traffic level is higher than the purchased Service Level and the customer has not purchased an extended DDoS Protection add-on license, the Customer will either immediately pay the Supplier for the observed attack traffic as a traffic add-on, or immediately pay the Supplier for extended DDoS Protection add-on. If the Customer does not act on any one of the above options, the Supplier shall be entitled to terminate the Service. A termination of the Service by Supplier as above, shall not absolve the Customer of its payment obligation for the entire Service term.

4. Supplier's Obligations

4.1. The Supplier agrees to supply the Service in accordance with the terms of this Agreement.

4.2. The Service will be implemented by the parties during the Onboarding Period as follows: (i) the Supplier will define a VIP for each Serviced Asset; (ii) the Customer will define a DNS record to the Supplier's VIP; (iii) the Supplier will define and tune the security policy; and (iv) the Customer and Supplier will run the Service Validation Procedure. During the Onboarding Period the Service will not be available; however, traffic availability issues will be handled in accordance with the Support Service SLA described in Appendix 2.

4.3. The Service will commence no sooner than successful completion of the Service Validation Procedure.

4.4. Billing of the Customer for the Service shall commence immediately upon submission by the Customer of a Purchase Order ("Order").

4.5. Regular maintenance work performed on the Supplier's Cloud Infrastructure shall only be performed during specific periods. These regular maintenance windows are scheduled on the 1st day of each calendar month and run between 00:00 and 06:00 hours in the time zone in which a specific Supplier's Cloud Infrastructure is located. During these regular "Maintenance Windows," the Supplier will make available an alternate Cloud Infrastructure to deliver the Service. If the Supplier needs to conduct non-Emergency Maintenance work outside of a scheduled regular Maintenance Window, it will do so after having provided the Customer with seven (7) days written notice about the work and the potential for interruption to the Service. For purposes of this Agreement, "Emergency Maintenance" means any activity that the Supplier, at its sole discretion, deems necessary to avert a situation that poses an immediate risk to the continued operation of the Service. The Supplier shall not be obligated to inform the Customer in advance of Emergency Maintenance work.

4.6. Supplier acknowledges and agrees that Supplier is the Data Processor of the Customer's Personal Information that is transmitted to Supplier's Cloud Infrastructure and as such Supplier will comply with its obligations as Data Processor under the Privacy & Data Security Laws and, where applicable, pursuant to Supplier's Data Protection Code of Conduct.

5. Customer's Obligations

The Customer acknowledges and agrees:

5.1. To order Service by submitting an Order. Each Order is hereby incorporated into, and made subject to, the terms of this Agreement.
5.2. To disclose to the Supplier all information that the Supplier requests so as to enable it to configure the Service.
5.3. To access the Service only through the interfaces and protocols provided or authorized by the Supplier and to not share the Customer's registration information (including the Customer's user name and password) with any third party for any purpose. The Customer agrees that the Customer will not access the Service through unauthorized means.

5.4. To protect the information on the Customer's computers such as by installing anti-virus software, updating the Customer's applications, password-protecting the Customer's files, and

not permitting third-party access to the Customer's computer systems.

5.5. To keep a copy of the content on the Customer's website for back-up purposes. In this regard, the Customer acknowledges and agrees that the Supplier does not warrant that it will maintain a back-up copy of the Customer's data on the Supplier's servers and that the Supplier is not a back-up service.

5.6. To comply with the terms, conditions and requirements of Appendix 3 in the event the Customer orders the CDN Service described in Appendix 2.

5.7. To execute a Service Validation Procedure together with the Supplier to ensure that the Service is configured appropriately to safeguard the Customer's Serviced Assets.

5.8. Customer will notify the Supplier in writing about any new Serviced Assets and/or about any planned configuration or content changes in any Serviced Assets. In any such event, the Customer agrees to execute a new Service Validation Procedure as shall be instructed by the Supplier, following which the Service will be retested against the new and/or reconfigured Serviced Asset. Once the retesting process is completed successfully, the Supplier will issue a new Service Validation Approval Notice to the Customer.

5.9. The Customer shall be responsible for all hardware, networks, communication devices, and other technology necessary to enable the Customer to access and/or use any Service provided hereunder.

5.10. The Customer acknowledges and agrees that the CDN Service is not protected by the Supplier by the Web Application Security module or by the DDoS Protection module described above and in Appendix 2.

5.11. To purchase all components of the Service (as defined and described in the Glossary) with the same service end date.

5.12. The Customer acknowledges, agrees and consents that in order to make the Service continuously available for the Customer and in order to maintain the Service Levels committed to by Supplier in this Agreement, the Supplier may need to transmit the traffic directed to the Customer's Serviced Assets, including transmission of Personal Information, to the Supplier's Cloud Infrastructure located outside of the country or outside of the continent in which the Customer is located. The Customer agrees that the Supplier may do so at its sole discretion, without first notifying the Customer of any such transmission and without having to obtain the Customer's or any third party's separate and specific consent for any such transmission. The Customer further acknowledges and agrees that the Customer is the Data Controller of the Customer's Personal Information and as such the Customer will comply with its obligations as the Data Controller under the Privacy & Data Security Laws, including, without limitation, providing any required notices and obtaining any required consents for the potential cross-border transmissions of Personal Information described above. Customer further acknowledges and agrees that Supplier is the Processor of the Customer's Personal Information that is successfully transmitted to Supplier's Cloud Infrastructure and authorizes Supplier to engage other Processors for carrying out processing activities on behalf of the Customer.

5.13. Customer Content; Traffic Rerouting

5.13.1. The Customer acknowledges and agrees that the Supplier may cache on its servers documents, information and/or any content and/or metadata and/or anything that can be accessed, received, transmitted, stored, processed or used (whether actively or passively),

including any form of information, audio, image, computer program or other functionality contained on the Customer's website and/or trafficked to the Customer's website ("**Customer Content**"), including without limitation rerouting Customer Content and all traffic directed to the Customer's website to another Supplier's designated IP address, for the purpose of enabling the provision of the Service. The Customer hereby grants the Supplier a non-exclusive, worldwide, fully paid-up, royalty-free license to receive, use, host, transfer, display and modify certain elements of the Customer's Content, in any media formats, solely for the purpose of enabling the provision of the Service. The foregoing license will apply to any form, media, or technology now known or hereafter developed.

5.13.2. The Customer hereby warrants and represents that: (i) the Customer is the sole owner of and/or hold all rights in and to the Customer Content; (ii) there are no restrictions or limitations that prevent or restrict the Customer from granting the Supplier the license rights above, and the Customer has obtained all authorizations, permits and certifications required under any applicable law (including applicable privacy and data security laws) to transfer the Customer Content to the Supplier and to grant the Supplier the above license rights; (iii) the Customer Content uploaded, posted, transmitted, processed or otherwise made available by the Customer will not constitute an Abuse (as defined below); (iv) the Customer Content is free of any digital rights management, including any software designed to limit the number of times the Customer Content may be copied or played; and (v) the Customer Content does not otherwise contain materials that violates any laws, rules, regulations or policies of any competent jurisdiction. Notwithstanding anything to the contrary in this Agreement, the Supplier may disallow the use of the Service when the Customer Content is flagged or blocked at the Supplier's sole discretion without any prior notice. The Customer will have no complaint, claim or demand towards the Supplier regarding the deletion, blocking or removal of the Customer Content the Customer created, contributed to or used. The Customer agrees to indemnify and defend the Supplier from and against any and all claims, causes of action (including discovery actions or subpoenas where the Supplier is not a party), liabilities, costs and expenses, including reasonable attorneys' fees, relating to or arising from breach by the Customer of its representations, warranties and covenants set forth in this Section.

5.14. As a prerequisite for provision of the Service, the Customer will ensure that all traffic to the Customer's website will be rerouted to the applicable IP address as set forth in the applicable Supplier Setup Form and by doing so the Customer shall fully comply with all ICANN rules and regulations and any internet registrar procedures in connection therewith. The Customer shall be solely responsible for rerouting such traffic back to the Customer's original IP address upon termination/expiration the Service.

6. Intellectual Property

6.1. Except for the limited rights expressly granted herein, this Agreement does not transfer to the Customer any Supplier Technology, and all right, title and interest in and to the Supplier Technology will remain the sole property of the Supplier. The Supplier and Customer each agrees that it will not, directly or indirectly, reverse engineer, decompile, disassemble or otherwise attempt to derive source code or other trade secrets of the other party.

7. Payments

7.1. Subject to the terms and conditions of this Agreement, the Customer agrees to pay the Supplier directly or through the Supplier's distribution channels all fees due in accordance with the agreed upon payment terms. All payments shall be made in US dollars.

8. Remedies

8.1. **General Service Outage or Serviced Asset Outage**

The Customer shall be eligible for remedies if affected by a General Service Outage or by a Serviced Asset Outage and it reports the interruption in the Service or the Serviced Assets to Supplier within five (5) calendar days of the commencement of the Service Outage event or the Serviced Asset Outage event. The Supplier shall determine by its sole discretion exercising good faith whether the interruption to the Service or the Serviced Assets caused a General Service Outage or a Serviced Asset Outage using its records, data and other evidence. For clarity, it is acknowledged by the Parties, that CDN Service Level failures are covered and will be compensated pursuant to this Section only if the CDN Service Level failure results in a General Service Outage. Remedies to the Customer for valid General Service Outage or Serviced Asset Outage claims will be in the form of additional Service days, to be provided at the end of the Service Term, as follows:

General Service Outage/Serviced Asset Outage Occurrence	**General Service Outage/Serviced Asset Outage Duration**	**Remedy**
Single event within a calendar month	More than 30 minutes but less than 3 hours	2 days credit of monthly Service per General Service Outage/Serviced Asset Outage
Single event within a calendar month	More than 3 hours but less than 72 hours	3 days credit of monthly Service per General Service Outage
Multiple events within 3 calendar months	Events greater than 45 minutes (at least one event in any 10 days)	Material Breach – Customer can terminate the Service

8.2. **Remedies Applicable to The DDoS Protection Module Only**

8.2.1. **Time-To-Mitigation and Consistency-Of-Mitigation Failures**

The following table describes the remedies should the Supplier fail to meet its Consistency-Of-Mitigation commitments (as defined in Appendix 2 with respect to the DDoS Protection module) following the Time-To-Mitigation target period (as defined in Appendix 2 with respect to the DDoS Protection module) within any given calendar month. Remedies to the Customer pursuant to this Section 8.2.1 will be in the form of additional Service days, to be provided at the end of the Service Term, as follows:

Time-To-Mitigation Duration (Per attack) or Failure to Provide Consistency-Of-Mitigation	Remedy
Greater than TTM target and less than 90 minutes	1 day credit of monthly Service
Greater than/equal to 90 minutes and less than 180 minutes	3 days credit of monthly Service
Greater than/equal to 180 minutes	4 days credit of monthly Service

8.3. **General Remedy Terms (applicable to all types of Service)**

8.3.1. The foregoing Service credits shall not be applicable during the first 21 days of operation following the initiation of the Service.

8.3.2. In order to qualify for any remedies, the Customer must be in good financial standing with the Supplier with all accounts current.

8.3.3. In order to qualify for remedies and subject to Sections 8.1 and 8.2 above, the Customer must have successfully completed a Service Validation Procedure within the previous twelve months.

8.3.4. To receive a credit under this Agreement, the Customer must (i) notify the Supplier within three (3) business days from the time the Customer becomes eligible to receive such credit, and (ii) provide the Supplier any such information regarding the event the Customer believes gives rise to the entitlement to such credit as the Supplier may request. The Customer shall forfeit its right to receive the Credit if it fails to comply with these requirements.

8.3.5. The Customer shall be entitled to only a single credit should any one incident result in a failure of more than one of the Service Level commitments.

8.3.6. The sum of credits for multiple events under either Section 8.1 or Section 8.2 or under both shall not exceed 25% of the monthly Service days for any single calendar month.

8.3.7. In the event that a General outage or a Serviced Asset Outage occurs as a result of a Special Unavailability event, the occurrence shall not qualify for remedial credits.

8.3.8. ANY CREDITS AWARDED BY THE SUPPLIER HEREUNDER SHALL BE THE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY FOR ANY FAILURE BY THE SUPPLIER TO MEET ANY SERVICE LEVEL AND ANY OTHER FAILURE, UNAVAILABILITY, DEGRADATION OR NONPERFORMANCE OF ANY SERVICE, INCLUDING, TO THE EXTENT APPLICABLE, ANY OUTAGES OR NETWORK CONGESTION.

9. Duration and Termination

9.1 This Agreement will commence on the date of the Customer's Order for the Service and, unless terminated sooner pursuant to the terms hereof, will last for 24 months (the "**Initial Term**").

9.2 At the end of the Initial Term, this Agreement will renew for successive terms of one (1) year (each a "**Renewal Term**") unless cancellation by a party is received in writing by the other party at least ninety (90) days before the expiration of the Initial Term or the then-current Renewal Term (as applicable). The Initial Term and all Renewal Terms will be referred to herein collectively as, the "Term".

9.3 Service Suspension

9.3.1 The Supplier may suspend or terminate the Service at its sole discretion if:

9.3.1.1 An Abuse has taken or is taking place as determined by the Supplier at its sole discretion;

9.3.1.2 Any of the In Excess Service Plan occurrences described in Section 3 has taken or is taking place; and/or

9.3.1.3 The Customer is in breach or default of its payment obligations to the Supplier, directly or through the Supplier's distribution channels;

9.3.1.4 The Customer is otherwise in material breach of this Agreement.

9.4 The Supplier may terminate the Agreement in the event that the Supplier cannot maintain any required regulatory approvals and/or data security standards, despite its reasonable efforts to do so, and pay back any prepaid amounts.

9.5 The Supplier may temporarily suspend any Service immediately in the event the Supplier has a good faith belief that such a course of action is reasonably necessary to mitigate material damage or liability that may result from the Customer's continued use of the Service. Following such an event, the Supplier shall restore the Service as quickly as reasonably possible and provide the Customer with a credit for the time the Service was unavailable.

9.6 Either Party may terminate this Agreement, upon written notice to the other Party, if the other Party is subject to proceedings in bankruptcy or insolvency, voluntarily or involuntarily, if a receiver is appointed with or without the other Party's consent, if the other Party assigns its property to its creditors or performs any other act of bankruptcy, or if the other Party becomes insolvent and cannot pay its debts when they are due.

9.7 In addition to any other rights and remedies available to it, either Party may immediately terminate this Agreement in the event of a material breach by the other Party of its obligations hereunder, including any of the representations, warranties and covenants hereunder, provided that such breach is not cured within thirty (30) days business days of notification of such breach.

9.8 In the event of any expiration or termination of any Service, the Customer's access to the applicable Service will end and the Supplier shall not be responsible for assisting the Customer with any transition to an alternative provider. In case the Supplier will not receive the Service subscription fees, the Supplier shall be entitled to terminate the Service and permitted to seek any remedy under applicable law.

11. Limitations of Liability

The Supplier and its sub-contractors/processors shall not be liable to any person, including any third party, for any special, indirect, incidental or consequential damages, including, but not limited to, lost profits from any cause whatsoever, loss of information, any claims alleging violations of any privacy right or any Privacy & Data Security laws, interruption of business and any other damage or loss arising from or in any way connected with the Service, even if the Supplier has been advised of the possibility of such damage or loss. Without derogating from the foregoing, in no event shall Supplier's and Supplier's sub-contractors'/processors' liability exceed the amounts actually paid by the Customer to Supplier under this Agreement.

12. Governing Law and Forum

This agreement shall be governed by and construed in accordance with the laws of Israel without regard for its conflicts of law provisions. Any dispute or disagreement arising under this Agreement shall be referred exclusively to the courts having subject matter jurisdiction and located in the city of Tel Aviv, Israel.

13. Waiver of Breach

The failure of either party to demand execution of any of the terms of this Agreement, or the waiver by either party of any breach under this Agreement shall not prevent a subsequent enforcement of such terms, nor be deemed a waiver of any subsequent breach.

14. Integration and Severability

In the event that any provision contained in this Agreement shall for any reason be held to be unenforceable in any respect under the laws of any government, such lack of enforceability shall not affect any other provision of this Agreement, but this Agreement shall be construed as if such unenforceable provision had not been contained herein.

15. Notices

All notices, requests, demands, and other communications under this Agreement shall be in writing and shall be deemed to have been duly given if mailed by registered mail prepaid, within 10 working days from the date they were mailed to the parties at the following addresses, or at such other address as may be given in writing in the future by either party to the other.

	Supplier:	Customer:
Company Name:	**Radware Ltd.**	**<Customer Name>**
Address:	22 Raoul Wallenberg Street, Tel-Aviv Israel 6971917	<Customer Address>

16. Execution

This Agreement shall not be binding upon either party until an officer of both organizations has executed it.

IN WITNESS HEREOF, THE PARTIES HERETO HAVE EXECUTED THIS AGREEMENT.

	Supplier:	Customer:
Company Name:	**Radware Ltd.**	**<Customer Name>**
Name:		
Title:		
Date:		
Signature:		

Appendix 1: Glossary

Term / Acronym	Definition
Abuses	The Customer agrees (on behalf of itself and/or any Customer representatives) to use the Service for lawful purposes only. Without limiting the foregoing, the following shall be deemed impermissible uses of the Service ("Abuses") and each shall constitute a breach of this Agreement by the Customer: (a) causing, aiding, encouraging, or facilitating a domain or URL hosted by the Supplier for the Customer (or any Customer end user) to point to or otherwise direct traffic or any material in violation of any applicable law or regulation; (b) for the Customer to use or encourage, aid or facilitate the use of the Service (including by pointing to websites or locations) to (i) create, transmit, distribute or store material that: violates trademark, patent, copyright, trade secret or other intellectual property laws; violate the privacy, publicity or other personal rights of others; (ii) include tools designed for compromising security (including but not limited to password guessing programs, cracking tools or network probing tools); (iii) violate export control, data protection or anti-terrorism laws of the U.S. and/or of any other applicable jurisdiction; (iv) impair the privacy of communications; (v) upload, post, transmit, process or otherwise make available any Customer Content that may be unlawful, harmful, tortuous, libelous, obscene, pornographic, contain sexually suggestive or explicit content, harassing, threatening, abusive, invasive of another's privacy, discriminatory based upon race, gender, color, creed, age, sexual orientation, disability or otherwise, racially or ethnically offensive, which encourages hatred against an identifiable group; which disparage, defame, or discredit the Supplier or any third person; which is defamatory or distasteful or which knowingly contains viruses; or constitutes a criminal offense or gives rise to civil liability; (c) use of the Service in a manner that directly or indirectly negatively affects the Supplier or the Supplier's network (including, without limitation, overloading servers on the Supplier's network or causing portions of the the Supplier's network to be blocked) or that directly or indirectly negatively affects the performance of other customers' websites; (d) any attempt by the Customer to penetrate or manipulate, or encourage, aid or facilitate the penetration or manipulation of, the security features of the Supplier network or any other system (including but not limited to unauthorized access to or use of data, systems or networks; probing, scanning or testing the vulnerability of a system or network; breaching security authentication measures; unauthorized monitoring of data or traffic; interference with the service of any user, host or network by any means; forging any TCP/IP packet header or any part of a message header); (e) posting article(s) or substantively similar articles(s) to an excessive number of newsgroups using a Supplier hosted domain or posting such messages through a Service; (f) sending unsolicited and/or mass e-mailings, whether or not such activities provoke complaints from the recipients (The Supplier has a zero tolerance policy on the sending of SPAM, junk e-mail or unsolicited commercial e-mail, and e-mail may not contain forged headers or fake contact information); (g) unauthorized access to or use of data, systems or networks, including any attempt to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without express authorization of the owner of the system or network; (h) unauthorized monitoring of data or traffic on any network or system without express

	authorization of the owner of the system or network; (i) utilizing an excessive amount of Supplier network resources without reasonable commercial justification; (j) interfering with or disrupting the Service or servers or networks connected to the Service, or disobeying any requirements, procedures, policies, or regulations of networks connected to the Service, (k) using the Service as an online storage space, including the storage or caching of a disproportionate percentage of pictures, movies, audio files, or other non-HTML content, or (l) breaching any other provision of this Agreement.
Application	The Customer's web application that is being protected by the Service. An Application entity in the Service can group multiple domains as long as they are (1) Deployed on the same origin server, (2) Share the same SSL certificate, (3) Share the same protection policy, and (4) Use the same character set.
Customer Equipment	Means the Customer's computer, telecommunications and other hardware and equipment.
Customer Technology	Means the Customer's proprietary technology, including the Customer's internet operations design, content, software tools, hardware designs, algorithms, software (in source and object forms), user interface designs, architecture, class libraries, objects and documentation (both printed and electronic), trade secrets and any related intellectual property rights throughout the world (whether owned by the Customer or licensed to the Customer from a third party) as of the Effective Date, and also including any derivatives, improvements, enhancements or extensions of the Customer Technology conceived, reduced to practice, or developed, during and after the term of this Agreement solely by the Customer.
Data Controller	Means as such term or like term is defined in the Privacy & Data Security Laws.
Data Protection Code of Conduct	Supplier's Data Protection Code of Conduct attached hereto as Appendix 4.
Data Processor	Means as such term or like term is defined in the Privacy & Data Security Laws.
DDoS Attack	Means a Distributed Denial of Service Attack that targets the Customer's Application at the network and application level such as UDP Floods, ICMP Floods, SYN Floods, TCP Flag Abuses, GET Floods, POST Floods.
Degraded Availability of Serviced Assets	Refers to a period of more than 60 continuous minutes during which, as a result of an attack, the Service fails to perform as designed and Customer IT assets – including but not limited to internet connectivity, website(s), servers, and applications – exhibit degraded performance. The determination of whether or not there exists or existed a Degraded Availability of Serviced Assets shall be made by the Supplier at its sole and absolute discretion.
Emergency Response Team (ERT)	Radware's Emergency Response Team is a service that is designed to provide 24x7 security services for customers facing a denial-of-service (DoS) attack or a malware outbreak. Radware's Emergency Response Team will provide instantaneous, expert security assistance in order to restore network and service operational status.

Content Delivery Network (CDN)	A content delivery network or content distribution network (CDN) is a globally distributed network of proxy servers deployed in multiple data centers. The goal of a CDN is to serve content to end-users from the users nearest location to provide better availability and better performance.
Force Majeure	Means acts or events beyond either party's reasonable control. Force Majeure may include, by way of example but not limitation, those circumstances beyond the control of the affected such as acts of God, the public enemy, acts of government, or any governmental department or agency thereof, as well as fire, flood, earthquakes, epidemics, quarantines, riots, wars, civil insurrections, freight embargoes.
General Service Outage	Means an event at which access to Serviced Assets through the Supplier's Cloud Infrastructure is completely unavailable while at the same time the Serviced Assets are fully available when accessed directly.
In Excess of The Service Plan Policy	The event when the calculated Legitimate Traffic level is higher than the level defined by the service plan as specified in the Customers' Order.
Legitimate Traffic Level	Means bandwidth based on 95th percentile calculation of network traffic targeted at the Serviced Assets through the Supplier's Cloud Infrastructure during non-attack periods as monitored by the Service monitoring facilities – to compute the 95th percentile value. The Supplier shall gather samples of traffic usage towards the protected Application, both inbound and outbound, at 5-minute intervals. The Supplier shall discard the highest 5% of the samples for each of inbound and outbound traffic, and the next highest sample becomes the 95th percentile value for the data set. For clarity, in case the Customer purchases the CDN Service, the above will be measured based on traffic incoming the Supplier's Cloud Infrastructure supporting the CDN Service.
Onboarding Period	Means the period commencing on the date the Customer requests in writing to include or add new domain(s) to the list of Serviced Assets and ending at a successful completion of the Service Validation Procedure for such additional domains.
Personal Information	Shall have the meaning of such term or like terms set forth in the Privacy & Data Security Laws.
Privacy & Data Security Laws	Means all applicable privacy and data protection laws, rules, regulations, best practices and regulatory guidance relating to privacy, data security, cybersecurity and Personal Information.
Service	The services ordered by the Customer from the Available Services described in Appendix 2, as set forth in one or more Orders.
Service Level	Means with respect to all Service Components the Service Uptime set forth in Section 2.1 above and, respectively with regard to each Service ordered by the Customer, the Service Level for such Service as set forth in Appendix 2 (if any).

Service Validation Procedure	The process by which the Service is tested against Customer's Serviced Assets.
Serviced Assets	Means the set of the Customer's serviced objects that are being protected by the Service, such as: Applications and their origin servers, websites and domain names.
Serviced Asset Outage	Means an interruption in accessing the Serviced Assets as a result of Supplier's actions or failures that results in: i. The total lack of availability of Serviced Assets for a period of at least 30 minutes; or ii. Degraded Availability of Serviced Assets for a period in excess of 1 hour.
Special Unavailability	Refers to an outage event of the Service due to: i. Network unavailability, including telecommunications failures that are used to connect the Supplier's Cloud Infrastructure to the Customer's Serviced Assets; or ii. scheduled maintenance, emergency maintenance or necessary upgrades; or iii. Problems with the Customer's domain name registrar; or iv. Problems with the Serviced Assets; or v. Customer Abuse; or vi. Other negligent or unlawful acts by the Customer or its agents or its suppliers; or vii. The Customer's use of the Service after Supplier advised the Customer to modify its use of the Service, if the Customer did not modify its use as advised; or viii. Any other action or inaction by the Customer or a third party; or ix. a Force Majeure; or x. With regard to the CDN Service- the SLA Exceptions set forth in Appendix 3. The cause of such an outage event shall be determined in good faith by Supplier
Supplier Technology	Means the Supplier's proprietary technology, including the Service, software tools, hardware designs, algorithms, software (in source and object forms), user interface designs, architecture, class libraries, objects and documentation (both printed and electronic), network designs, trade secrets and any related intellectual property rights throughout the world (whether owned by the Supplier or licensed to the Supplier from a third party) as of the Effective Date, and also including any new developments, derivatives, improvements, enhancements or extensions of any Supplier proprietary technology that are conceived, reduced to practice, or developed during and after the term of this Agreement by either party.
Supplier's Cloud Infrastructure	Refers to cloud-based data center facilities operated by or on behalf of the Supplier in order to deliver the Service or any part thereof including, without limitation, any third-party data centers.

Verizon	Means a Verizon entity with which the Supplier has contracted to utilize the CDN service offered by such an entity in providing to the Customer the CDN Service described in Appendix 2 and Appendix 3.

Appendix 2: Detailed Service Features

1. Web Application Firewall Module Features

The following table lists the available Web Application Firewall features per package:

Application Attack Protection	**Enterprise**	**Enterprise Premium**
Injections: SQL, OS and LDAP	Yes	Yes
Cross Site Scripting	Yes	Yes
Cross Site Request Forgery	Yes	Yes
Predictable Resource Location	Yes	Yes
Remote File Inclusions	Yes	Yes
Brute Force Attacks	Yes	Yes
Buffer Overflow	Yes	Yes
Information Leakage	Yes	Yes
Improper Output Handling	Yes	Yes
Directory Indexing	*Yes*	*Yes*
Access Control (White and Black list, Geolocation, anonymous proxies)	Yes	Yes
Known Vulnerabilities and Custom Rules	Yes	Yes
Session Hijacking	Yes	Yes
Cookie Manipulation and Poisoning	Yes	Yes
HTTP Protocol Manipulation	Yes	Yes
XML and Web Services Attacks	Yes	Yes
Anti-scrapping (IP-Agnostic Fingerprinting)	Yes	Yes

2. DDoS Protection Module Features

The following table lists the available DDoS Protection features per package:

DDoS Protection Offering	**Enterprise**	**Enterprise Premium**
Behavioral network layer DDoS protection	Yes	Yes
Behavioral application layer DDoS protection	Yes	Yes
Network Challenge Response	Yes	Yes
HTTP Challenge Response	Yes	Yes
Access List – on demand up to 1 list per month	Up to 100 entries	Up to 100 entries
Weekly Security Update Subscription	Yes	Yes
Attack volume supported	1G included, scalable on-demand*	1G included, scalable on-demand*

***** Applies in all Radware POPs excluding Azure-based POPs where DDoS protection is delivered per Azure offering.

3. Content Delivery Network Module Features

The following table lists the available CDN features per package:

CDN Offering	Enterprise	Enterprise Premium
Global CDN	Yes	Yes
Static caching	Yes	Yes
HTTP compression	Yes	Yes
Purge cache	Yes	Yes
Load fresh content on demand	Yes	Yes
Real time analytics	Yes	Yes
Traffic volume supported	According to purchased plan	

4. Managed Service Features

4.1. Managed Service is available in two packages:

Service offering	Enterprise	Enterprise Premium
24x7 support	Yes	Yes
Managed security service	Yes	Yes
Emergency response attack mitigation	Yes	Yes
Logs review and system monitoring	Yes	Yes
Weekly calls during onboarding phase	Yes	Yes
Monthly security event reports	Yes	Yes
Technical Account Manager	No	Yes
Forensics reports (two per year)	No	Yes
Pre-attack high risk alerts	No	Yes
Post-attack alerts and recommendations	No	Yes
Monthly call following monthly report	No	Yes
ERT direct “Hot-Line”	No	Yes
Dedicated Security Expert*	No	Yes
High risk event identification and engagement*	No	Yes
ERT record of security configuration*	No	Yes
Application security policy review and optimization	Upon Application onboarding	Proactively
DDoS protection policy review and optimization	Upon Application onboarding	Proactively
Point of contact	TAC	Direct to ERT
Time-to-security-expert response SLA	30 min	10 min
Periodic security assessment configuration review	Yearly	Quarterly

**Items relevant for customer with Extended DDoS protection (DDOS Add-On)*

4.2. Customer Support Service

Cloud Services Severity Case Classifications

When a support case is first opened, a classification rating is assigned based on problem severity, complexity, system availability, and business impact. There are four severity levels:

- **Business Critical** – Emergency/Network Down or function failure, operations are severely restricted

- **Major** – Major Impact Sustained. Service does not operate as designed or a limited problem condition exists. An acceptable workaround is available

- **Minor** – Minor Impact Sustained. Minor condition or configuration issue is present but can be avoided or there is a question or issue related to the documentation or other general inquiry.

- **Policy Changes at Customer's Initiative** – Policy changes requested by the Customer within the scope of the Service, including adding a new protection (such as adding a Brute Force protection in the Gold offering set), removing an existing protection, or modifying the settings of an existing protection (such as changing the number of allowed unsuccessful login attempts in the Brute Force protection mode).

Note: When a service request is created with a Business Critical severity, the on-call TAC manager is immediately notified and an appropriate resource is allocated.

Note of Clarification: Policy changes or policy tunings required to remedy false positives will not be considered a Policy Change at the Customer's Initiative, but rather will be classified as one of the other Severity Case Classifications above, depending on the applicable problem severity, complexity, system availability, and business impact.

Response Times (during business and off business hours)
The table below summarizes typical response times for service requests based on severity level:

Severity	Suggested Reporting Method	Response Time
Business Critical	• Phone	• <30 minutes
Major	• E-mail, Online or iSupport[1]	• Within 24 hours
Minor	• E-mail, Online or iSupport[5]	• Within 24 hours
Policy Changes at Customer's Initiative	• E-mail	• Next Business Day

[1] Response time is within one business day if the request is submitted in English. Requests submitted in any other language must first be translated and may exceed the one-business-day response time.

Radware Technical Support Services includes 24x7x365 support. Support is delivered by our nine (9) centers around the world. This means that during business hours your service request will be typically addressed by the Radware TAC (Technical Assistance Center) in your home region.

Support during off business hours, including weekends and regional public holidays, is covered 24x7x365 via the Radware Global TAC for cases categorized as Business Critical.

Radware TAC provides 24x7x365 support as long as you make resources available that allow 24x7 interactions. Cases are seamlessly transferred between Radware Global TACs following-the-sun, to ensure cases are worked on continually for rapid resolution.

Technical Team Overview
Radware Technical Support consists of two tiers of support, all staffed by Radware Engineers.

Team	Role
TAC	• Works all support cases • Direct Enterprise customers interaction
ERT	• Works all support cases • Direct Enterprise Premium customers interaction
CloudOps	• Works all support cases escalated by TAC engineers • Direct customer interaction

TAC is the initial point of contact and addresses 92% of all customer inquiries. Questions range from service capabilities through security policy false positives and configuration issues. These teams are primarily located in the US, India, and Israel.

CloudOps handles all product related issues that require onboarding of new customers and new domains, advanced policy changes, complex case handling testing or possible resolution by Research & Development (R&D).

Appendix 3: CDN Service Attachment

Appendix 3- CDN Service Attachment.d

Appendix 4: Data Protection Code of Conduct

Radware Data
Protection Code of