Master Cloud Services Agreement

UNLESS SPECIFICALLY SET FORTH OTHERWISE IN A SIGNED AGREEMENT BETWEEN YOU (“YOU” OR “CUSTOMER”) AND RADWARE LTD./ RADWARE INC. (“SUPPLIER”), THIS AGREEMENT WILL APPLY TO ANY SALE/PURCHASE TRANSACTION FOR THE SERVICE(S). DEFINITIONS OF CAPITALIZED TERMS ARE IN THE GLOSSARY.

YOU AGREE TO BE BOUND BY THE TERMS OF THIS AGREMEENT EITHER BY YOUR EXPRESS AGREEMENT TO THIS AGREEMENT OR BY USING THE SERVICE(S).

IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THE TERMS OF THIS AGREEMENT, IN WHICH CASE THE TERMS "YOU" "YOUR" AND “CUSTOMER” SHALL REFER TO SUCH ENTITY. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH THE TERMS OF THIS AGREMEENT, DO NOT USE THE SERVICE(S).

1. **Services**. Each Service available for purchase under this Agreement is described in a CSS which contains certain Service-specific terms and conditions. This Agreement applies to all Services ordered by Customer from Supplier under this Agreement directly or through an Approved Source. During the term of this Agreement, Supplier shall provide the Services to Customer pursuant to this Agreement and the applicable CSS.

2. **Term of Service**. The initial term of a Service will last from the Service Start Date for the period indicated in the initial Purchase Order for the Service (the “**Initial Service Term**”). At the end of the Initial Service Term and thereafter, the Service will automatically renew for the same term or such other term as set forth in the Purchase Order (each, a "**Renewal Service Term**"), unless (a) the Customer notifies Supplier or if applicable its Approved Source 60 days in advance of the end of the then-current Service Term of its desire not to renew the Service, or (b) Customer or the Approved Source elect not to auto-renew at the time of the initial Purchase Order placed with the Supplier or Approved Source. Prior to the expiration of the then-current Service Term, and with reasonable advance notice, Supplier will notify Customer or where applicable, its Approved Source, in writing of the Service fees for the Renewal Service Term. The time period covered by the Initial Service Term and all Renewal Service Terms with respect to a Service is referred to collectively herein as the “**Service Term**.” Service extensions and add-ons will expire together with the expiration of the Service to which they relate.

3. **Term of Agreement**. This Agreement will become effective as of the Effective Date and, unless terminated sooner in accordance with the terms below, will remain in effect for as long as there are ongoing Services (including suspended Services). Once the last Service ordered hereunder expires or is terminated, this Agreement will concurrently automatically expire or terminate. Provisions that survive termination or expiration of this Agreement are those relating to payment, Warranties, Intellectual Property, IP Indemnification, Limitations of Liability, Term of Agreement, Confidentiality, General and others which by their nature are intended to survive.

4. **Suspension and Termination Rights**.

4.1. Supplier may suspend or terminate any Service hereunder in its sole discretion after a fourteen (14)-day advance notice, if: (**i**) an Acceptable Use Policy violation has taken or is taking place as determined by Supplier in good faith; and/or (**ii**) an Excessive Use has taken or is taking place and an Excess Fee is not timely paid therefor in accordance with Section 9 below, or the Excessive use is not stopped within the above notice period; and/or (**iii**) Supplier cannot maintain any required regulatory approvals, despite its reasonable efforts to do so, in which case Supplier will pay back any prepaid amounts for the suspended/terminated Service Term. Service suspension or termination pursuant to sections (i) or (ii) will not absolve Customer of its payment obligations for the entire Service Term.

4.2. Either Party may terminate this Agreement upon (**i**) written notice to the other Party, if such 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; and/or (**ii**) in the event of a material breach by the other Party of its obligations, representations, warranties or covenants hereunder (including, without limitation, payment obligations), provided that such breach is not cured prior to, or within thirty (30) days of, notification of such breach.

5. **Financial Terms**. The financial terms including pricing, invoicing and payment terms will be as agreed between Customer and Supplier or Supplier's Approved Source. Supplier will start invoicing the Customer or its Approved Source for a Service from the applicable Service Start Date. All payments shall be made in US dollars unless specifically agreed otherwise in the Purchase Order as accepted by Supplier. Fees for Services are exclusive of any taxes. Customer will pay Supplier or its Approved Source any sales, value-added or other similar taxes imposed by applicable law on the Services ordered by the Customer, except for taxes based on Supplier's income.

6. **Service Onboarding**. The parties agree to conduct a Service onboarding as detailed in the CSS (the "**Service Onboarding**"). The Service Onboarding will be deemed completed upon the occurrence of the Onboarding Completion Milestone (as defined in the applicable CSS), the date of which will be the "**Service Production Date**". Unless specifically set forth otherwise in a particular CSS, Service Level commitments set forth in any CSS will apply only as of the Service Production Date.

7. **Service Maintenance and Support**. Details of technical maintenance and support for a Service are described in the applicable CSS.

8. **Customer's Obligations and Acknowledgements.** Customer: (**i**) agrees to use all Services solely pursuant to this Agreement and solely for Customer's direct benefit and, unless otherwise agreed in writing with Supplier, will not assign or resell access to a Service to a third party outside of Customer's enterprise, or combine any Service with Customer's value add to create a commercially available Customer branded solution that Customer markets to its end user customers; (**ii**) grants Supplier the right to host, process, display and transmit the Customer Content for the sole purpose of providing the Service pursuant to and in accordance with this Agreement; (**ii**) has sole responsibility for the Customer Content, and for obtaining all rights and consents related to the Customer Content and required for Supplier to perform the Service; (**iii**) to the extent the Service includes CPE(s), Customer shall provide

Supplier with access to and, if necessary, allocate externally accessible IP addresses to such CPE to facilitate the operation of the Service; (i**v**) may access a Service only to the extent purchased by the Customer unless the Customer or its Approved Source pays an Excess Fee for an Excessive Use; (**v**) is responsible for use of the Service by any user who accesses the Service with Customer's account credentials; (**vi**) agrees that, except as set forth otherwise in the applicable CSS, Service Levels will apply to newly provisioned or changed Protected Assets only once a Service Onboarding is completed for such Protected Assets; and (**vii**) acknowledges and agrees that Supplier may (a) derive, compile and create in the course of its provision of the Service, including its use of Customer Content in connection therewith, certain aggregated analytical data which does not contain Personal Data ("**Aggregate Data**") and (b) use such Aggregate Data solely for internal purposes (including the improvement of Supplier's solutions) not prohibited by applicable law.

9. **Excessive Service Use**. In the event of an Excessive Use that is visible to and can be monitored by the Customer, or where Supplier informs Customer of the Excessive Use, then, in any such event, if Customer does not stop the Excessive Use as required by Supplier in the notice provided under Section 4.1 above, Supplier or Supplier's Approved Source will invoice Customer an Excess Fee. Customer agrees to pay any invoice for Excess Fee according to the payment terms required by Supplier (or Supplier's Approved Source) for same.

10. **Acceptable Use Policy**. Customer may not, and may not cause or permit others to: (a) use the Service in violation of any applicable law or regulation or in such a manner that renders or is likely to render the Supplier to violate any applicable law or regulation; (b) perform Excessive Use that gives Supplier a right to suspend or terminate the Service pursuant to Section 4.1 above; (c) use the Service in a way contrary to its intended purpose (for example, collaborating with hackers to generate attacks against the Customer) (the items listed in subsection (a)-(c), the "**Acceptable Use Policy**"). In addition to other rights that Supplier may have in this Agreement, Supplier has the right to take remedial action if the Acceptable Use Policy is violated, and such remedial action may include, without limitation, removing or disabling access to materials that violate the Acceptable Use Policy as well as notifying the appropriate law-enforcement agencies of the violation. Additionally, in the event of a violation by Customer of the Acceptable Use Policy, Supplier shall not be liable for any resulting consequences including failure to meet any Service performance metrics. Customer agrees to cooperate with Supplier to resolve any Acceptable Use Policy violations.

11. **Data Protection**. Customer is the Data Controller of Personal Data to the extent included in any Customer Content, and Supplier is the Data Processor acting on behalf of the Customer pursuant to this Agreement and as further specified in the applicable Data Processing Profile. Supplier and Customer will each comply with its respective obligations as Data Processor/Data Controller under applicable Applicable Data Protection Laws and, where applicable, pursuant to the Radware DPA. Customer authorizes Supplier to engage other Processors for carrying out processing activities on behalf of the Customer, including the sub-processors listed at https://www.radware.com/documents/cloud-subprocessors/.

12. **Changes**.

12.1. Supplier may modify components of any Service (to the extent such change is made to the generally available Service) and, in such event, upon thirty (30) days' notice; provided that Customer

or its Approved Source may terminate the applicable Purchase Order without termination charge if Supplier fails to remedy a material decrease in the functionality of the affected Service within thirty (30) days of written notice from Customer.

12.2. Supplier may discontinue a Service on six (6) months' notice and in this case Supplier will continue to provide the Service for the remainder of Customer's unexpired Service Term or work with Customer to migrate to another Supplier Service offering.

13. **Warranties**. EXCEPT FOR THE SERVICE LEVEL WARRANTIES IN THE SLA: (**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. NEITHER RADWARE NOR ITS APPROVED SOURCES WARRANT THAT ALL SECURITY THREATS AND VULNERABILITIES WILL BE DETECTED AND/OR MITIGATED BY THE SERVICES OR THAT THE PERFORMANCE OF THE SERVICES WILL RENDER THE CUSTOMER'S SYSTEMS INVULNERABLE TO SECURITY BREACHES. EXCLUSIVE REMEDY FOR FAILURE OF ANY WARRANTY IS REPAIR OF THE SERVICE OR A PRO RATA REFUND OF PURCHASE PRICE IN SUPPLIER'S SOLE DISCRETION.

14. **Intellectual Property**. Except for the limited rights expressly granted herein, this Agreement does not transfer to the Customer any right in any Service nor to any component thereof or any methodologies relating thereto. All rights, title and interest in and to the Services and in and to Aggregate Data will remain the sole property of the Supplier and all rights, title and interest in and to Customer Content will remain the sole property of the Customer and its customers. 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.

15. **IP Indemnification**. Supplier will defend any claim or threatened claim against Customer that Customer's valid use of a Service infringes a third party's patent, copyright or registered trademark (an "**IP Claim**") and will indemnify Customer against the final non-appealable judgment entered by a court of competent jurisdiction or any settlements arising out of an IP Claim, provided that Customer: (i) promptly notifies Supplier in writing of the IP Claim; (ii) fully cooperates with Supplier in the defense of the IP Claim; and (iii) grants Supplier the right to exclusively control the defense and settlement of the IP Claim and any subsequent appeals. Supplier will have no obligation to reimburse Customer for attorney fees and costs incurred prior to Supplier's receipt of notification of the IP Claim. Customer, at its own expense, may retain Customer's own counsel. If an IP Claim occurs, or if Supplier reasonably believes a claim is likely to occur, Supplier will either procure for Customer the right to continue using the Service, or replace or modify the Service with functionality that is at least equivalent. If Supplier determines that those alternatives are not reasonably available, upon Supplier's notice, Customer's right to use the affected Service will terminate and Customer will cease using the Service and Supplier will return any fees received by Supplier for the remaining Service Term. Supplier has no obligation with respect to any IP Claim based on: (a) the amount or duration of use made of the Service, revenue Customer earned, or services Customer offered; (b) combination, operation, or use of the Service with non-Supplier products, software or business processes or (c) any Service provided on a no charge, beta or evaluation basis. This Section 15 states Supplier's sole and exclusive obligation and Customer's exclusive remedy for IP Claims.

16. **Limitations of Liability**. Neither party shall be liable to the other party or to any third party, for any special, indirect, incidental or consequential, exemplary or reliance damages, losses or expenses (including without limitation, loss of profits, loss of information, loss or corruption of data, loss or interruption of business) arising from or in any way connected with the parties' obligations under this Agreement, however caused, and whether based on contract, tort (including negligence), equity or other theory of liability whatsoever, even if such party has been advised of the possibility of such damages or losses or expenses. Without derogating from the foregoing, except for liability for payments for the Services, in no event shall a party's total aggregate liability to the other party exceed the amounts actually paid to Supplier for the Service that is the subject matter of the claim during the twelve (12) month period preceding the damaging event. This section will survive the termination/expiration any sale/purchase document between Radware and Customer. Notwithstanding the foregoing, none of the exclusions and limitations in this section shall apply in respect of (i) liability in negligence causing personal injury or death; (ii) liability for fraudulent misrepresentation; or (iii) any other liability which cannot by law be excluded or limited (as appropriate). The foregoing limitations and exclusions apply collectively to a party and such party's affiliates, suppliers, sub-contractors, sub-processors and, in the case of Radware, its resellers, distributors, OEMs and other Approved Sources.

17. **Confidentiality**. Each party shall treat confidentially the terms and conditions of this Agreement, all information relating to the Services and the transactions contemplated under this Agreement and all information provided by each party to the other regarding its business and operations. All confidential information provided by a party hereto shall remain the property of the disclosing party and shall be used by the receiving party solely for the purpose of rendering or obtaining Services pursuant to this Agreement and, except as may be required in carrying out this Agreement, shall not be disclosed to any third party without the prior consent of the disclosing party. The foregoing shall not be applicable to any information that is publicly available when provided or thereafter becomes publicly available other than through a breach of this Agreement, or that is required to be disclosed by or to any regulatory authority, or by judicial or administrative process or otherwise by applicable law.

18. **Order of Priority of Documents**. The following documents will prevail in the following order of priority: (**i**) a CSS; (**ii**) the body of this Agreement; (**iii**) a Purchase Order. Notwithstanding the foregoing, where a DPA is required under applicable Applicable Data Protection Laws, the DPA applies and prevails over any conflicting terms of the above listed documents. Supplier shall not be bound by any terms and conditions which may be part of the Purchase Order or any other offer or document, whether oral or written, which attempt to impose any terms and/or conditions that are additional, conflicting or inconsistent with this Agreement; unless this Agreement specifically allows the inclusion in any such document of additional, conflicting or inconsistent terms and/or conditions (e.g. payment terms).

19. **General**. (**i**) This Agreement shall be governed and construed in accordance with the substantive laws of, and venue will be located in: (a) Israel if Customer is located in Israel; (b) England and Wales if Customer is located in EMEA; (c) Singapore if Customer is located in APAC; and (d) the state of New York for all other Customer locations; (**ii**) Neither the license to use the Services nor this Agreement are assignable or transferable by Customer without prior written notice to, and written consent from, Supplier; any attempt to do so shall be void; (**iii**) 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; (**iv**) 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; (**v**) Except for payment obligations, neither party shall be liable to the other, nor be deemed to be in default under, or in breach of any provision of, this Agreement for the nonperformance or delay in performance of any of such party's obligations when such nonperformance or delay is due to Force Majeure Events. "**Force Majeure Events**" means: (a) acts of God, (b) flood, fire, earthquake, tornado, tsunami, storm or explosion, (c) war, invasion, riot, or other civil unrest, (d) pandemics, epidemics, or quarantine restrictions, (e) government regulations or orders, (f) action by any governmental authority, (g) national or regional emergency, (h) strikes, labor stoppages or slowdowns or other industrial disturbances, (i) shortage of adequate power or transportation facilities, or (j) any other event which is beyond the reasonable control of such party. The party suffering a Force Majeure Event shall give notice of such Force Majeure Event as soon as reasonably practicable to the other party; (**vi**) All notices or other communications required hereunder shall be made in writing and shall be deemed to be effectively given: **(a)** when made available to Customer by Supplier posting such notice to the Supplier's Service Portal, and if emailed, the first business day after sending the notice (provided that Supplier's Service Portal or email shall not be sufficient for legal notices, including notices of Service or Agreement termination, alleged breach or an indemnifiable IP Claim); or **(b)** if hand delivered, when received, and if mailed for overnight delivery, when delivery by the overnight carrier is made; in each instance at the applicable address set forth below, and with respect to legal notices, to Attn: Legal Department (for Supplier- legal_all@radware.com):

Glossary

"Agreement" means this Master Cloud Services Agreement, the CSSs thereunder, the DPA and any other documents referenced herein.

"Applicable Data Protection Laws" means, as the case may be, data protection laws addressing the safeguarding and lawful processing of Personal Data that apply to the Services ordered by Customer hereunder, including, if Customer resides in an EU member country, EU General Data Protection Regulation 2016/679 and complementary data protection laws in EU member countries.

"Approved Source" means a reseller, distributor or systems integrator authorized to sell the Services to Customer.

"**Cloud Infrastructure**" means the computer hardware and software (including, without limitation, software applications, software interfaces, operating system and databases), storage capacity and all other resources (including, without limitation, telecommunications equipment and third-party data centers and hosting facilities) used by Supplier to make the Services available to, and usable by, Customer.

"CSS" or "Cloud Service Schedule" means the document defining the specific terms and conditions that apply to each Service ordered by the Customer.

"Customer Content" means all text, files, documents, information, data (including Personal Data) and other material, in any format and as applicable to the purchased Service, provided by Customer or by Customer's users that reside in, or run on or through, the Cloud Infrastructure.

"Customer Premises Equipment (CPE)" means equipment (hardware and/or software) situated in facilities owned or used by the Customer.

"Data Controller" and "Data Processor" means as such terms or like terms are defined in the Applicable Data Protection Laws, or if not defined in the Applicable Data Protection Laws, 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data; and 'processor' means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

"**Data Processing Agreement**" or "**DPA**" means Supplier's global data processing agreement that forms an integral part of this Agreement where required under applicable Applicable Data Protection Laws and available at https://www.radware.com/documents/dpa-customer/.

"**Data Processing Profile**" means, with respect to each Service, the Data Processing Profile attached as Schedule A to the DPA.

"**Excess Fee**" means an additional Service fee invoiced by Supplier to Customer or the Approved Source for an Excessive Use according to Supplier's price list or written agreement with the Customer or Approved Source which is the price difference between the level of Service ordered by the Customer and the level of actual use of the Service by Customer.

"Excessive Use" means an event where the Customer's actual usage of a Service exceeds the level ordered by Customer such as, but not limited to (by way of example only and as and if applicable to the purchased Service), limitations on traffic level (legitimate or attack, as applicable), the number of traffic diversions, duration of traffic diversions, number of Protected Assets, the maximum number of virtual machine instances monitored by the Service or any other limitations.

"Onboarding Completion Milestone" means with regard to a particular Service, as defined in the CSS for that Service.

"Personal Data" means as the meaning ascribed to "personally identifiable information," "personal information," "personal data" or equivalent terms as such terms are defined under Applicable Data Protection Laws.

"Protected Assets" means with regard to a particular Service, the set of IT assets owned by/hosted for the Customer (including in public clouds), that are served or protected by the Service, such as by way of example only but without limitation, objects, network segments and servers, public cloud managed services, applications and their origin servers, websites and domain names, individual IP addresses and IP networks.

"**Purchase Order**" means a purchase order or other document indicating the Services purchased by the Customer that is submitted by Customer or an Approved Source to Supplier and is accepted in writing by Supplier by issuing an order confirmation or by activating and/or delivering the Service.

"**Service**" means a cloud-based service offered by Supplier on its price list as updated from time to time and ordered by Customer from Supplier or an Approved Source in a Purchase Order.

"**Service Level**" means each of the performance criteria set forth in the Service Level Agreement.

"**Service Level Agreement**" or "**SLA**" means with regard to a particular Service, the part of the applicable CSS that describes the performance criteria with regard to the underlying Service and the remedies for failing to meet same.

"Service Start Date"[1] means with regard to a particular Service, the date that is the later of (i) three business days after of the date of receipt by Supplier of the Purchase Order for the Service or (ii) the date specified in the Purchase Order, which in no event shall be longer than 90 days from the date of receipt of the Purchase Order for the Services.

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

[1] Given that immediately upon submission of a Purchase Order (or closely thereafter at the latest), Supplier allocates resources and is prepared to fully provide the Services ordered, a Service will start three business days after the date of the initial Purchase Order for the Service.

Cloud DDoS Protection: Service Schedule

THIS CLOUD SERVICE SCHEDULE ("**CSS**") is supplemental to a Master Cloud Services Agreement ("**MSA**") between Radware Ltd./Inc. ("**Supplier**") and the entity that has accepted or executed the MSA ("**Customer**"). This CSS sets forth Service-specific terms and conditions that govern orders placed by

Service Description

Customer for Supplier's **Cloud DDoS Protection Service** (the "**Service**"). Capitalized terms used in this CSS but not defined herein shall have the meanings ascribed to them in the MSA.

The Service is a cloud-based service designed to protect data centers, networks and servers against Distributed Denial of Service (DDoS) Attacks, by providing multi-vector DDoS attack detection and mitigation, at the network- and application-layer.

The Service is powered by a global cloud security network with dedicated Scrubbing Centers spread globally. The Customer's traffic is being redirected from the Protected Assets (such as data centers, networks or servers) to the Service, which receives Customer's traffic through its Scrubbing Centers. In the Scrubbing Center, the Customer's traffic is inspected and cleaned of malicious DDoS attack traffic, where the remaining clean (legitimate) traffic is directed back to the Customer's Protected Assets.

The Service features a Service Portal which provides visibility and self-service management of the Service elements.

Service Flavors

The Service can be deployed in either a *cloud-only* or a *hybrid* deployment mode.

The Service can be consumed in either an a*lways-on* or an o*n-demand* usage mode.

The combination of deployment mode (cloud-only / hybrid) and usage mode (always-on / on-demand) forms four (4) offering categories, where each addresses different Customer needs and mandates specific Service terms.

The following table summarizes the available offering options, divided into the applicable Service offering categories:

Offering Categories		Usage Model	
		On-Demand *Traffic is redirected through the Cloud DDoS Scrubbing Center upon a DDoS attack*	**Always-on** *Traffic is regularly redirected through the Service Scrubbing Centers*
Deployment Model	**Cloud-only** *Cloud-based DDoS protection service*	***Cloud On-demand offerings:*** • On-demand Cloud DDoS Protection Service	***Cloud Always-on offerings:*** • Always-on Cloud DDoS Protection Service
	Hybrid *Cloud-based DDoS protection service operates in conjunction with on-prem DDoS mitigation device*	***Hybrid On-demand offerings:*** • On-demand Hybrid DDoS Protection Service	***Hybrid Always-on offerings:*** • Always-on Hybrid DDoS Protection Service

Service Onboarding

An Onboarding Process is considered completed once it reaches the Onboarding Completion Milestone. In order to qualify for the Service Levels below on any Protected Asset, the Customer must complete the Onboarding Process for any such Protected Asset. For more information on Service onboarding process, please refer to the **Cloud DDoS Onboarding Guide** available at https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=6126c375-78f8-40bb-a304-3d1fc759e068

Service Levels

The following table lists the service level per Solution Offering:

Service Level		Offering Category Applicability			
Metric	**Case**	**Cloud On-demand**	**Cloud Always-on**	**Hybrid On-demand**	**Hybrid Always-on**
	Under Diversion	Sub-second	Sub-second	Sub-second	Sub-second

Service Level		Offering Category Applicability			
Metric	**Case**	**Cloud On-demand**	**Cloud Always-on**	**Hybrid On-demand**	**Hybrid Always-on**
Time-to-Detect *per method*	CPE Attack Detection	NA	NA	5 min	5 min
	Flow Monitoring	10 min	NA	NA	NA
	No Monitoring	NA	NA	NA	NA
Time-to-Notification *(Programmatic / Human)*		2 / 15 minutes	2 / 15 minutes	2 / 15 minutes	2 / 15 minutes
Time-to-Initiate Diversion *(Programmatic / Manual)*		1 / 15 minutes	NA	1 / 15 minutes	NA
Time-to-Mitigate Attack *per protection*		Seconds	Seconds	Seconds	Seconds
Consistency-of-Mitigation		95%	95%	95%	95%
Service Availability		99.999%	99.999%	99.999%	99.999%
Service Portal Availability		99.9%	99.9%	99.9%	99.9%

Each of the Time-To-Detect, Time-To-Notification and Time-to-Initiate Diversion commitments applies only if the Customer enables the automatic detection, notification and diversion capabilities of the Service.

Supplier shall not be deemed to have failed a Service Level in the event the failure is due to conditions that are beyond Supplier's control such as, but without limitation, Customer's internet connectivity, Customer's firewall settings and any other systems outside of Supplier's control that may block or delay

the Customer's access to data or the receipt of email or phone calls, phone and cellular line conditions, no answer of a call by the Customer, etc.

Service Remedies

In the event of Availability Incident, the Customer may be eligible for Availability Credits in the form of additional Service days, to be provided at the end of the Service Term, as follows:

Availability Incident Occurrence	Availability Credit
Single event, less than 3 hours - per calendar month	1 day credit of monthly Service per Availability Incident for affected Protected Data Center(s)
Single event, more than 3 hours but less than 72 hours - per calendar month	3 days credit of monthly Service per Availability Incident for affected Protected Data Center(s)
Multiple events, each more than 45 minutes, with at least one event in any 10 days - within 3 consecutive calendar months	Material Breach – Customer can terminate Service for affected Protected Data Center(s)

The Customer needs to comply with the following terms in order to be eligible to submit a Claim:

a. Log a support ticket for each Availability Incident with Supplier's Customer Support for the Service, in accordance with Supplier's procedures for reporting Severity 1 support issues, and within twenty-four (24) hours of Customer's first becoming aware of the Availability Incident.
b. Provide all reasonable information about the Availability Incident and about the Claim and reasonably assist Supplier with the diagnosis and resolution of the Availability Incident to the extent required by Supplier.
c. Submit a Claim no later than five (5) business days after the Customer becoming aware of the Availability Incident that is the subject of the Claim.

Supplier will follow the below guidelines for Availability Credit calculation:

a. Supplier will use its reasonable judgment to validate Claims based on information available in Supplier's records, which will prevail in the event of a conflict with data in the Customer's records.
b. The sum of Availability Credits for multiple events in a particular Protected Data Center shall not exceed 25% of the monthly Service days for that Protected Data Center for any single calendar month.

c. Availability Credits will be provided only on Protected Assets that have reached the Onboarding Completion Milestone .
d. THE AVAILABILITY CREDITS PROVIDED TO CUSTOMER IN ACCORDANCE WITH THIS CSS ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND SUPPLIER'S SOLE LIABILITY WITH RESPECT TO ANY CLAIM AND WITH RESPECT TO ANY FAILURE BY SUPPLIER TO MEET ANY SERVICE LEVEL.

Support Level

Technical Support for the Service is available to Customer to assist in its use of the Service, as follows:

- ERT Standard support - included in the subscription of all offerings.
- ERT Premium support - unless stated otherwise in the part numbers and their descriptions listed in the Purchase Order, ERT Premium support subscription is available for an additional charge.

For more information on Support Level options and metrics per product offering, please refer to the **ERT Service Guide** available at :https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=bc348fe1-e90c-4e30-9d64-1d903006efa5.

The below table describes the Case Severity and associated Response Time:

Severity	**Response Time**	**Severity Criteria**
P1 – Business Critical	30 minutes—available for customers of ERT Standard 10 minutes—available for customers of ERT Premium	Emergency/network down. Use of services is completely suspended. No workaround is available. **Example:** A major degradation of system or service performance that impacts service quality or significantly impairs network-operator control or operational effectiveness. The overall network is degraded causing severe limitations to operations or network-management software. The product has a major feature that is not working properly and has only a difficult workaround.
P2 – Major	1 business day	Major impact sustained. The Service does not operate as designed, or a limited problem condition exists. An acceptable workaround is available. **Example:** A problem that results in a condition that seriously affects system operation, maintenance and administration, and so on, and requires immediate attention. The urgency is less than in a business-critical situation because of a lesser immediate or impending effect on system performance, customers, business operation, or revenue.
P3 – Medium	1 business day	Medium impact sustained.

		Example: The Service does not operate as designed or a limited problem condition exists, but the product's main functionality is not affected.
P4 – Minor	1 business day	Minor impact sustained. The issue does not significantly impair the functioning of the system and does not significantly affect service to customers. These problems are tolerable during system use. **Example:** A minor condition or configuration issue is present but can be avoided, or there is a question or issue related to documentation or some other general inquiry.

Definitions

"**Always-on Service**" means a Service flavor where all of the Customer's traffic directed at the Protected Assets is routed continuously through the Scrubbing Centers, keeping the Customer protected against both volumetric and non-volumetric DDoS Attacks and additional threats.

"**Availability Credit**" means the remedy Supplier will provide for a validated Claim. The Availability Credit will be applied in the form of additional Service days, to be provided at the end of the Service Term.

"**Availability Incident**" means an interruption of the Service as a result of Supplier's failure to meet any of the Service Levels (as defined in the section above) that directly results in:

1) the total lack of availability of Protected Assets for a period of at least 5 minutes; or
2) Degraded Availability of Protected Assets for a period in excess of 1 hour.

A Service interruption will not be considered an Availability Incident if it results from the following:

- Scheduled Maintenance;
- in cases in which the Customer was not routing traffic to the Supplier's Scrubbing Center(s) or no Customer traffic was affected by the Availability Incident;
- Network unavailability outside of Supplier's Scrubbing Centers, including telecommunications failures that are used to connect the Protected Assets to the Scrubbing Centers;
- Force Majeure;
- Problems with the Customer's domain name registrar.
- Customer's or and third party's acts, inactions or omissions (including anyone gaining access to the Service by means of Customer's passwords or equipment);
- Negligent or unlawful acts or omissions by Customer or its agents or its suppliers.

The cause of such Availability Incident shall be determined in good faith by Supplier.

"**Behavioral DoS (BDoS) Protection**" means protection method where clean traffic is forwarded while attack traffic is blocked. The protection kicks-in when anomaly is identified. BDoS protection is a Radware's patent-protected real-time signature creation technology, which continuously models "normal behavior" of network, application, and user.

"**Claim**" means a claim for Availability Credit(s).

"**Consistency-of-Mitigation**" means the proportion of the clean (legitimate) traffic of a Protected Asset forwarded from the Scrubbing Center to the Protected Data Center, out of the total traffic forwarded. The Consistency-Of-Mitigation measurement window is defined as the period that starts when the Time-To-Mitigate Service Level starts and until the End of Attack.

"Customer Premises Equipment (CPE)" means Radware DefensePro device deployed in the Customer's on-prem Protected Data Center.

"**Degraded Availability of Protected Assets**" means a period of more than 60 continuous minutes during which, as a result of a DDoS Attack, the Protected Assets exhibit degraded performance. The determination of whether or not there exists or existed a Degraded Availability of Protected Assets shall be made by Supplier and Customer exercising good faith.

"**Distributed Denial of Service (DDoS) Attack**" means an attack that targets one or more of the Customer's Protected Assets.

"**End of Attack**" means the time at which an attack is judged to have been aborted. The precise time is deemed to be when inbound internet link utilization levels drop to 65% or below and/or when they drop to a level below Customer's typical inbound internet link utilization levels for the time of day and day of week, whichever link utilization level is higher.

"**Filter Protection**" means a protection method where all traffic meeting filter criteria is blocked. Filters may refer to traffic filters or signatures.

"**Flow Monitoring"** means analyzing the data provided using NetFlow, a capability allowing to collect IP network traffic as it enters or exits an interface.

"**Hybrid Service**" means a Service flavor where the Customer is provided with DDoS Attack mitigation coverage through high-capacity cloud-based DDoS protection, which complements and integrates with Supplier's on-premises DDoS protection device. This includes monitoring of the customer's on-premise DDoS protection devices for security alerts.

"**On-demand Service**" means a Service flavor where attack traffic is redirected to the Scrubbing Centers when under a DDoS Attack. During peace time, the traffic is directed to the Protected Data center, while the Service includes the option for monitoring the customer's on-premises equipment for traffic flow data in order to detect DDoS Attacks.

"Onboarding Completion Milestone" occurs upon a traffic redirection of >95% of the protected traffic from its origin to the applicable Scrubbing Center, for at least one Protected Asset per each Protected Data Center.

"**Onboarding Process**" means a process in which the Customer provides all needed parameters in order to provision and protect its Protected Assets by the Service. This process involves configurations both at the Service end and at the Customer's end and is described in detail in Supplier's **Cloud DDoS Onboarding Guide** abaliable at: https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=6126c375-78f8-40bb-a304-3d1fc759e068

"**Portal-Availability**" means the proportion of time the Service Portal (or its specific components) is available, calculated annually.

"**Protected Assets**" mean a set of Customer's protected objects, network segments and servers including but not limited to domain names, individual IP addresses and IP networks, which are

protected by the Service and have been and have been successfully onboarded to the Service through the completing of an Onboarding Process.

"**Protected Data Center**" means a unique data center that can be protected by the Service. A protected data center hosts Protected Assets, extending to network or servers, and can be owned by the Customer or operated by a 3rd party (e.g. colocation provider, public cloud provider, etc.). Each protected data center is registered to the Service by adding its configuration to the Service Portal.

"**Rate-based Protection**" means protection method where traffic mix is forwarded up to limit.

"**Service-Availability**" means the proportion of time the Service (or its specific components) is available, calculated annually.

"**Service Level**" means each of the service levels as described in the Service Levels section of this CSS.

"**Service Portal**" means a Customer-facing Web application which provides data, reports and self-service capabilities relevant to the Protected Assets.

"**Scheduled Maintenance**" means any preventative, routine or scheduled maintenance that is performed on the Supplier's facilities or any component used to deliver the Service thereof, (a) for which Supplier provides Customer notice at least 7 days in advance by email, or (b) recurring weekly maintenance window every Sunday between 7:00 AM EST and 9:00 AM EST. During this maintenance window the Service can be intermittently unavailable.

"**Scrubbing Center**" means a cloud-based data center facility operated by, or on behalf of, Supplier in order to deliver the Service.

"Time-To-Detect" means the amount of time in which the Service detects a DDoS Attack. The time to detect may vary based on detection method set by use case and customer preference.

"Time-To-Notification Programmatic" means the amount of time in which the Supplier notifies the Customer upon an attack detection, through a programmatic mean: API, Portal, Email, or SMS notification.

"**Time-To-Notification Human**:" means the amount of time in which the Supplier notifies the Customer upon an attack detection, through a phone call.

"**Time-To-Initiate-Diversion**" means the amount of time in which the Supplier initiates the diversion of traffic directed towards the Customer's Protected Assets that are under a DDoS Attack, to the Scrubbing Center.

"**Time-To-Mitigate Attack**" means the period starting since 75% or more of the Customer's traffic from the Protected Assets that are under a DDoS Attack, has been successfully diverted to the Scrubbing Centers, until reaching Consistency-Of-Mitigation. Time-To-Mitigate may re-commence when the DDoS Attack is morphed and/or when the Attack Vectors change and end when the Consistency-Of-Mitigation is reached.

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

Cloud DDoS Protection: Service Schedule – Peak Protection

THIS CLOUD SERVICE SCHEDULE ("**CSS**") is supplemental to a Master Cloud Services Agreement ("**MSA**") between Radware Ltd./Inc. ("**Supplier**") and the entity that has accepted or executed the MSA ("**Customer**"). This CSS sets forth Service-specific terms and conditions that govern orders placed by Customer for Supplier's **Cloud DDoS Peak Protection Service** (the "**Service**"). Capitalized terms used in this CSS but not defined herein shall have the meanings ascribed to them in the MSA.

Service Description

The Service is a cloud-based service designed to protect data centers, networks and servers 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. The Customer's traffic is being redirected from the Protected Assets (such as data centers, networks or servers) to the Service, which receives Customer's traffic through its Scrubbing Centers. In the Scrubbing Center, the Customer's traffic is inspected and cleaned of malicious DDoS attack traffic, where the remaining clean (legitimate) traffic is directed back to the Customer's Protected Assets.

The Service features a Service Portal which provides visibility and self-service management of the Service elements.

The Service is provided to carriers and managed security service provider's (MSSP) with extended DDoS protection capacity for mitigating massive DDoS attacks beyond their local DDoS scrubbing capacity, which have CPE unit.

Service Onboarding

An Onboarding Process is considered completed once it reaches the Onboarding Completion Milestone. In order to qualify for the Service Levels below on any Protected Asset, the Customer must complete the Onboarding Process for any such Protected Asset. For more information on Service onboarding process, please refer to the **Cloud DDoS Onboarding Guide** available at: https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=6126c375-78f8-40bb-a304-3d1fc759e068

Service Levels

The following table lists the service level per Solution Offering:

Service Level	Offering Category Applicability
Metric	**Peak Protection**
Time-to-Initiate Diversion *(Programmatic / Manual)*	1 / 15 minutes
Time-to-Mitigate Attack *per protection*	Seconds
Consistency-of-Mitigation	95%
Service Availability	99.999%
Service Portal Availability	99.9%

Supplier shall not be deemed to have failed a Service Level in the event the failure is due to conditions that are beyond Supplier's control such as, but without limitation, Customer's internet connectivity, Customer's firewall settings and any other systems outside of Supplier's control that may block or delay the Customer's access to data or the receipt of email or phone calls, phone and cellular line conditions, no answer of a call by the Customer, etc.

Service Remedies

In the event of Availability Incident, the Customer may be eligible for Availability Credits in the form of additional Service days, to be provided at the end of the Service Term, as follows:

Availability Incident Occurrence	Availability Credit
Single event, less than 3 hours - per calendar month	1 day credit of monthly Service per Availability Incident for affected Protected Data Center(s)
Single event, more than 3 hours but less than 72 hours - per calendar month	3 days credit of monthly Service per Availability Incident for affected Protected Data Center(s)

Multiple events, each more than 45 minutes, with at least one event in any 10 days - within 3 consecutive calendar months	Material Breach – Customer can terminate Service for affected Protected Data Center(s)

The Customer needs to comply with the following terms in order to be eligible to submit a Claim:

d. Log a support ticket for each Availability Incident with Supplier's Customer Support for the Service, in accordance with Supplier's procedures for reporting Severity 1 support issues, and within twenty-four (24) hours of Customer's first becoming aware of the Availability Incident.
e. Provide all reasonable information about the Availability Incident and about the Claim and reasonably assist Supplier with the diagnosis and resolution of the Availability Incident to the extent required by Supplier.
f. Submit a Claim no later than five (5) business days after the Customer becoming aware of the Availability Incident that is the subject of the Claim.

Supplier will follow the below guidelines for Availability Credit calculation:

e. Supplier will use its reasonable judgment to validate Claims based on information available in Supplier's records, which will prevail in the event of a conflict with data in the Customer's records.
f. The sum of Availability Credits for multiple events in a particular Protected Data Center shall not exceed 25% of the monthly Service days for that Protected Data Center for any single calendar month.
g. Availability Credits will be provided only on Protected Assets that have reached the Onboarding Completion Milestone .
h. THE AVAILABILITY CREDITS PROVIDED TO CUSTOMER IN ACCORDANCE WITH THIS CSS ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND SUPPLIER'S SOLE LIABILITY WITH RESPECT TO ANY CLAIM AND WITH RESPECT TO ANY FAILURE BY SUPPLIER TO MEET ANY SERVICE LEVEL.

Support Level

Technical Support for the Service is available to Customer to assist in its use of the Service, as follows:

- ERT Standard support - included in the subscription of all offerings.
- ERT Premium support - unless stated otherwise in the part numbers and their descriptions listed in the Purchase Order, ERT Premium support subscription is available for an additional charge.

For more information on Support Level options and metrics per product offering, please refer to the **ERT Service Guide** available at :
https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=bc348fe1-e90c-4e30-9d64-1d903006efa5

The below table describes the Case Severity and associated Response Time:

Severity	Response Time	Severity Criteria
P1 – Business Critical	30 minutes—available for customers of ERT Standard 10 minutes—available for customers of ERT Premium	Emergency/network down. Use of services is completely suspended. No workaround is available. **Example:** A major degradation of system or service performance that impacts service quality or significantly impairs network-operator control or operational effectiveness. The overall network is degraded causing severe limitations to operations or network-management software. The product has a major feature that is not working properly and has only a difficult workaround.
P2 – Major	1 business day	Major impact sustained. The Service does not operate as designed, or a limited problem condition exists. An acceptable workaround is available. **Example:** A problem that results in a condition that seriously affects system operation, maintenance and administration, and so on, and requires immediate attention. The urgency is less than in a business-critical situation because of a lesser immediate or impending effect on system performance, customers, business operation, or revenue.
P3 – Medium	1 business day	Medium impact sustained. **Example:** The Service does not operate as designed or a limited problem condition exists, but the product's main functionality is not affected.
P4 – Minor	1 business day	Minor impact sustained. The issue does not significantly impair the functioning of the system and does not significantly affect service to customers. These problems are tolerable during system use. **Example:** A minor condition or configuration issue is present but can be avoided, or there is a question or issue related to documentation or some other general inquiry.

Definitions

"**Availability Credit**" means the remedy Supplier will provide for a validated Claim. The Availability Credit will be applied in the form of additional Service days, to be provided at the end of the Service Term.

"**Availability Incident**" means an interruption of the Service as a result of Supplier's failure to meet any of the Service Levels (as defined in the section above) that directly results in:

3) the total lack of availability of Protected Assets for a period of at least 5 minutes; or
4) Degraded Availability of Protected Assets for a period in excess of 1 hour.

A Service interruption will not be considered an Availability Incident if it results from the following:

- Scheduled Maintenance;
- in cases in which the Customer was not routing traffic to the Supplier's Scrubbing Center(s) or no Customer traffic was affected by the Availability Incident;
- Network unavailability outside of Supplier's Scrubbing Centers, including telecommunications failures that are used to connect the Protected Assets to the Scrubbing Centers;
- Force Majeure;
- Problems with the Customer's domain name registrar.
- Customer's or and third party's acts, inactions or omissions (including anyone gaining access to the Service by means of Customer's passwords or equipment);
- Negligent or unlawful acts or omissions by Customer or its agents or its suppliers.

The cause of such Availability Incident shall be determined in good faith by Supplier.

"**Claim**" means a claim for Availability Credit(s).

"**Consistency-of-Mitigation**" means the proportion of the clean (legitimate) traffic of a Protected Asset forwarded from the Scrubbing Center to the Protected Data Center, out of the total traffic forwarded. The Consistency-Of-Mitigation measurement window is defined as the period that starts when the Time-To-Mitigate Service Level starts and until the End of Attack.

"Customer Premises Equipment ("CPE")" means Radware DefensePro device deployed in the Customer's on prem Protected Data Center.

"**Degraded Availability of Protected Assets**" means a period of more than 60 continuous minutes during which, as a result of a DDoS Attack, the Protected Assets exhibit degraded performance. The determination of whether or not there exists or existed a Degraded Availability of Protected Assets shall be made by Supplier and Customer exercising good faith.

"**End of Attack**" means the time at which an attack is judged to have been aborted. The precise time is deemed to be when inbound internet link utilization levels drop to 65% or below and/or when they drop to a level below Customer's typical inbound internet link utilization levels for the time of day and day of week, whichever link utilization level is higher.

Onboarding Completion Milestone" occurs upon a traffic redirection of >95% of the protected traffic from its origin to the applicable Scrubbing Center, for at least one Protected Asset per each Protected Data Center.

"**Onboarding Process**" means a process in which the Customer provides all needed parameters in order to provision and protect its Protected Assets by the Service. This process involves configurations both at the Service end and at the Customer's end and is described in detail in Supplier's **Cloud DDoS Onboarding Guide** Available at: https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=6126c375-78f8-40bb-a304-3d1fc759e068 .

"**Portal Availability**" means the proportion of time the Service Portal (or its specific components) is available, calculated annually.

"**Protected Assets**" mean a set of Customer's protected objects, network segments and servers including but not limited to domain names, individual IP addresses and IP networks, which are protected by the Service and have been and have been successfully onboarded to the Service through the completing of an Onboarding Process.

"**Protected Data Center**" means a unique data center that can be protected by the Service. A protected data center hosts Protected Assets, extending to network or servers, and can be owned by the Customer or operated by a 3rd party (e.g. colocation provider, public cloud provider, etc.). Each protected data center is registered to the Service by adding its configuration to the Service Portal.

"**Service Availability**" means the proportion of time the Service (or its specific components) is available, calculated annually.

"**Service Level**" means each of the service level as described in Service Levels section of this CSS.

"**Service Portal**" means a Customer-facing Web application which provides data, reports and self-service capabilities relevant to the Protected Assets.

"**Scheduled Maintenance**" means any preventative, routine or scheduled maintenance that is performed on the Supplier's facilities or any component used to deliver the Service thereof, (a) for which Supplier provides Customer notice at least 7 days in advance by email, or (b) recurring weekly maintenance window every Sunday between 7:00 AM EST and 9:00 AM EST. During this maintenance window the Service can be intermittently unavailable.

"**Scrubbing Center**" means a cloud-based data center facility operated by, or on behalf of, Supplier in order to deliver the Service.

"**Time-To-Initiate-Diversion**" means the amount of time in which the Supplier initiates the diversion of traffic directed towards the Customer's Protected Assets that are under a DDoS Attack, to the Scrubbing Center.

"**Time-To-Mitigate Attack**" means the period starting since 75% or more of the Customer's traffic from the Protected Assets that are under a DDoS Attack, has been successfully diverted to the Scrubbing Centers, until reaching consistency-Of-Mitigation. Time-To-Mitigate may re-commence when the DDoS Attack is morphed and/or when the Attack Vectors change and end when the Consistency-Of-Mitigation is reached.

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

Bot Manager Cloud Service: Service Schedule

THIS CLOUD SERVICE SCHEDULE ("**CSS**") is supplemental to a Master Cloud Services Agreement ("**MSA**") between Radware Ltd./Inc. ("**Supplier**") and the entity that has accepted or executed the MSA ("**Customer**"). This CSS sets forth Service-specific terms and conditions that govern orders placed by Customer for Supplier's **Bot Manager Service**. Capitalized terms used in this CSS but not defined herein shall have the meanings ascribed to them in the MSA.

1. SERVICE.

Supplier's Bot Manager Service provides protection to web applications, mobile apps and APIs from automated attacks using bots. The Service makes decisions to distinguish between the activity of human visitors, the activity of legitimate automated software systems (i.e., good bots) and the 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 access. The Service uses a number of proprietary techniques that are 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 protects against OWASP automated threats to Web, mobile and APIs.

The Service provides the flexibility to configure various bot mitigation options based on the bot generation, bot category, specific page URL, geography and source fingerprint. The Service also provides granular analytics and reporting functionality for customers through the Supplier's Service Portal.

The Service may be deployed either through a customer on-prem integrated agent, virtual appliance or a DNS diversion using a cloud service bundle.

Managed Service

Optionally, the Customer can purchase from Supplier the following managed service alternatives as part of Supplier's Service offering:

1 weekly hour – managed service	including Customer briefing, data scientist policy improvements and custom rules. Suitable for classified content and media and publisher apps.
2 weekly hours – managed service	including Customer briefing, data scientist policy improvements, custom rules and detailed custom reports. Suitable for e-commerce apps.
4 weekly hours – managed service	including Customer briefing, proactive protection policy data scientist reviews for improved protection, custom rules and detailed custom

	reports. Suitable for financial apps, high end e-commerce apps and smaller scale travel industry apps.
8 weekly hours – managed service	including proactive protection policy reviews for improved protection, custom rules and detailed custom reports. Suitable for high-end financial, travel industry, e-commerce and gaming apps.

2. SUPPORT.

During the Service Term, Supplier shall make available to Customer technical consultation and support relating to the operation of the Service via email and Supplier's online Support portal. Customer may request Support in any of the following ways:

For all Service deployments:

- Email: botmanager_support@radware.com
- Support Telephone Numbers: List of the global telephone directory for Radware Technical Support
- Online Chat: Available at the bottom right corner on Supplier's Bot Manager Service Portal

3. SERVICE LEVELS

Availability:

Supplier's Service Portal

- For all Service deployments, the Supplier's Service Portal will be available on a 99.9% of the time calculated on an annual basis.

Service Components

- For DNS diversion deployment:
  The Data Path Service component will be available on a 99.999% of the time calculated on an annual basis
- For Service deployments through a Customer on-prem integrated agent or virtual appliance:
  The API Endpoint will be available on a 99.999% of the time calculated on an annual basis.

Latency:

- Latency will be 100ms or less for the 95th percentile of API Endpoint requests.

For purposes of this Agreement the following terms shall have the following meanings:

"**Data Path**" means the infrastructure that receives and transmits the customer web traffic as a proxy between network clients and the protected applications.

"**Supplier's Service Portal**" means a Customer facing web-based application. The application displays Bot Manager Service data relevant to the Customer and allows the Customer to perform various Service configurations and utilize various functions.

"**API Endpoint**" means the infrastructure that exposes the API's that are utilized by the Bot Manager plugins, SDK's or other implementation components.

Support Service Response Times:

Support Service Response Times are summarized in the table below, based on severity level:

Severity	Suggested Reporting Method	Response Time
Business Critical	Phone	Within 30 minutes
Major	E-mail or Supplier's Online Support Service Portal	Within 1 Business Day
Minor	E-mail or Supplier's Online Support Service Portal	Within 1 Business Day
Policy Changes at Customer's Initiative	E-mail	Next Business Day
Requests submitted in any language other than English must first be translated and may exceed the one-business-day response time.		

Support Case Severity 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. Use of the Services is completely suspended. No workaround is available.
- **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. Issue that does not significantly impair the functioning of the system and does not significantly affect the Service. These problems are tolerable during Service use.

- **Policy Changes at Customer's Initiative** – Policy changes requested by Customer within the scope of the Service that cannot be done in a self-service manner.

North America

Radware Inc.

575 Corporate Drive

Mahwah, NJ 07430

Tel: +1-888-234-5763

International

Radware Ltd.

22 Raoul Wallenberg St.

Tel Aviv 69710, Israel

Tel: 972 3 766 8666

Cloud WAF: Service Schedule

THIS CLOUD SERVICE SCHEDULE ("**CSS**") is supplemental to a Master Cloud Services Agreement ("**MSA**") between Radware Ltd./Inc. ("**Supplier**") and the entity that has accepted or executed the MSA ("**Customer**"). This CSS set forth Service-specific terms and conditions that govern orders placed by Customer for Supplier's **Cloud WAF Service** (the "**Service**"). Capitalized terms used in this CSS but not defined herein shall have the meanings ascribed to them in the MSA.

Service Description

The Service is a cloud-based offering that is designed to protect web applications against a wide-range of web application layer attacks. The Service also features several add-on modules providing further capabilities (described in the Service Options below).

The Service is provided through a global network of distributed Points of Presence (PoPs), using an optimized and highly available architecture, securing the customer's Protected Assets from multiple PoP locations, to ensure that they are fully protected. The Service's PoPs are located at major traffic hubs with connections to tier-1 ISPs, striving for low latency and minimal impact on web applications' performance.

The Service features a Service Portal that provides visibility and self-service management of the Service elements.

The Service is offered by default with ERT Standard. For more information refer to the Support Level section below.

Service Options

The Service features the following components:

1. ***Cloud Web Application Firewall*** - the Service implements both Negative Security Model and Positive Security Model that provide detection and mitigation of web application and API attacks and the continuous fine-tuning of security policies in changing usage patterns.
2. ***Cloud Bot Manager add-on*** - allows protecting websites, APIs, and mobile applications against malicious bot traffic, using behavioral modelling for granular intent analysis, collective bot intelligence, and device fingerprinting. This module helps protect against account takeover, denial of inventory, card fraud, web scraping, and other OWASP Top 21 automated threats.
3. ***Volumetric Cloud DDoS Protection*** **add-on** - provides protection against volumetric DDoS attacks. DDoS protection of up to 1Gbps of attack traffic is included in the Service, except when provided through Azure-based PoPs where DDoS protection is provided by Azure. Add-ons for protection against DDoS attacks up to 10Gbps, and against DDoS attacks of unlimited size are also available.
4. ***Content Delivery Network (CDN) add-on*** – allows fast delivery of Web content to end users, ensuring better user experience and productivity at any location. Using a CDN allows savings on resources in the data center, by reducing bandwidth consumption and server utilization. It

uses a globally distributed network of high capacity, high speed cache servers, and leveraging advanced caching techniques.

5. ***Emergency Response Team (ERT) Premium Support*** - provides 24x7 proactive security services including policy tuning, vulnerability research, asset monitoring, and attack mitigation. For more information refer to the Support Level section below.

Service Onboarding

An Onboarding Process is considered completed once the Onboarding Completion Milestone occurs. In order to qualify for the Service Levels below on any Protected Asset, the Customer must complete the Onboarding Process for any such Protected Asset. For more information on Service onboarding process, please refer to the Cloud WAF Quick Start Guide available at : https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=d320bfdc-0588-4025-9343-00dd931d3201

Service Levels

The following table lists the service levels for the Service:

Metric	Value
Service Network Infrastructure Availability	99.999% of time measured on an annual basis
Service Portal Availability	99.9% of time measured on an annual basis

Supplier shall not be deemed to have failed a Service Level in the event the failure is due to conditions that are beyond Supplier's control such as, but without limitation, Customer's internet connectivity, Customer's firewall settings and any other systems that may block or delay the Customer's access to data.

Service Remedies

In the event of Availability Incident, the Customer will be eligible for Availability Credits in the form of additional Service days, to be provided at the end of the Service Term, as follows:

Availability Incident Occurrence	Availability Credit
Single event, less than 3 hours - per calendar month	1 day credit of monthly Service per Availability Incident for affected Protected Asset(s)
Single event, more than 3 hours but less than 72 hours - per calendar month	3 days credit of monthly Service per Availability Incident for affected Protected Asset(s)

Multiple events, each more than 45 minutes, with at least one event in any 10 days - within 3 calendar months	Material Breach – Customer may terminate the Service

The Customer needs to comply with the following terms in order to be eligible to submit a Claim:

a. Log a support ticket for each Availability Incident with Supplier's Customer Support for the Service, in accordance with Supplier's procedure for reporting Severity 1 support issues as described in the ERT Service Guide, and within twenty-four (24) hours of Customer's first becoming aware of the Availability Incident.
b. Provide all reasonable information related the Availability Incident and reasonably assist Supplier with the diagnosis and resolution of the Availability Incident to the extent required by Supplier.
c. Submit a Claim for Availability Credit no later than five (5) business days after the Customer becoming aware of the Availability Incident that is the subject of the Claim.

Supplier will follow the below guidelines for Availability Credit calculation:

a. Supplier will use its reasonable judgment to validate Claims based on information available in Supplier's records, which will prevail in the event of a conflict with data in the Customer's records.
b. The sum of Availability Credits for multiple events on a particular Protected Asset shall not exceed 25% of the monthly Service days for that Protected Asset for any single calendar month.
c. Availability Credits will be provided only on Protected Assets that have reached the Onboarding Completion Milestone.
d. THE AVAILABILITY CREDITS PROVIDED TO CUSTOMER IN ACCORDANCE WITH THIS CSS ARE CUSTOMER'S SOLE AND EXCLUSIVE REMEDY AND SUPPLIER'S SOLE LIABILITY WITH RESPECT TO ANY CLAIM AND WITH RESPECT TO ANY FAILURE BY SUPPLIER TO MEET ANY SERVICE LEVEL.

Support Level

Technical Support for the Service is available to Customer to assist in its use of the Service, as follows:

- Cloud WAF Enterprise with ERT Standard support - included in the subscription of all offerings.
- Cloud WAF Enterprise with ERT Premium support - unless stated otherwise in the part numbers and their descriptions listed in the Purchase Order, ERT Premium support subscription is available for an additional charge.

Metric		Cloud WAF	
		ERT Standard	*ERT Premium*
Eligibility	Included, no additional cost	YES	NO
	Preconditions	N/A	The Premium plan must apply to all Cloud products of the customer. Enterprise Premium is optional when ACV exceeds the ERT-Premium-Eligible fee.
	Mandatory	N/A	Premium is mandatory when ACV exceeds the ERT-Premium-Required fee.
Service hours		24x7x365	24x7x365
Support portal Access		✓	✓
Email support		✓	✓
Phone support for non-emergency, up to 30 minutes response time		✓	✓
Emergency hot-line service, up to 10 minutes response time			✓
Number of authorized customer contacts		5	Unlimited
Continuous asset-health monitoring		✓	✓
Onboarding assistance		✓	✓
Proactive automatic security anomaly alerts		✓	✓
Designated Customer Success Manager			✓
Periodic security status reporting			✓
Priority service case handling			✓
24x7 WAF-attack detection and alerts		✓	✓
Policy tuning and configuration management		On-demand	✓

The below table describes the Case Severity and associated Response Time:

Severity	Response Time	Severity Criteria
P1 – Business Critical	30 minutes—available for customers of ERT Standard 10 minutes—available for customers of the ERT Premium	Emergency/network down. Use of Services is completely suspended. No workaround is available. **Example:** A major degradation of system or Service performance that impacts Service quality or significantly impairs network-operator control or operational effectiveness. The overall network is degraded causing severe limitations to operations or network-management software. The Service has a major feature that is not working properly and has only a difficult workaround.
P2 – Major	1 business day	Major impact sustained. The Service does not operate as designed, or a limited problem condition exists. An acceptable workaround is available. **Example:** A problem that results in a condition that seriously affects system operation, maintenance and administration, and so on, and requires immediate attention. The urgency is less than in a business-critical situation because of a lesser immediate or impending effect on system performance, customers, business operation, or revenue.
P3 – Medium	1 business day	Medium impact sustained. **Example:** The Service does not operate as designed or a limited problem condition exists, but the Service's main functionality is not affected.

Severity	Response Time	Severity Criteria
P4 – Minor	1 business day	Minor impact sustained. The issue does not significantly impair the functioning of the system and does not significantly affect Service to customers. These problems are tolerable during system use. **Example:** A minor condition or configuration issue is present but can be avoided, or there is a question or issue related to documentation or some other general inquiry.

For more information on Support Level options and metrics per product offering, please refer to the **ERT Service Guide** available at: https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=bc348fe1-e90c-4e30-9d64-1d903006efa5.

Definitions

"Availability Credit" means the remedy Supplier will provide for a validated Claim. The Availability Credit will be applied in the form of additional Service days, to be provided at the end of the Service Term.

"**Availability Incident**" means an interruption of the Service as a result of Supplier's failure to meet any of the Service Levels (as defined in the section above) that directly results in:

1) The total lack of availability of Protected Assets for a period of at least 5 minutes.
2) Degraded Availability of Protected Assets for a period in excess of 1 hour.

A Service interruption will not be considered an Availability Incident if it results from the following:

- Scheduled Maintenance;
- Network unavailability outside of Supplier's PoPs, including failures of telecommunication resources that are used to connect the Protected Assets to the Supplier's PoPs.
- Force Majeure;
- Problems with the Customer's domain name registrar;Customer's or and third party's acts, inactions or omissions (including anyone gaining access to the Service by means of Customer's passwords or equipment);
- Negligent or unlawful acts by Customer or its agents or its suppliers.

The cause of such Availability Incident shall be determined in good faith by Supplier.

“Claim” means a claim submitted by Customer to Supplier pursuant to the Service Terms & Conditions when the Service Availability metric has not been met.

“**Degraded Availability of Protected Assets**” means a period of more than 60 continuous minutes during which, as a result of a DDoS Attack, the Service fails to perform as designed and the Protected Assets exhibit degraded performance. The determination of whether or not there exists or existed a Degraded Availability of Protected Assets shall be made by Supplier exercising good faith.

“Emergency Response Team (ERT)” means a team of experts in network and application cybersecurity threats with hands-on experience and skills to detect and mitigate attacks in real-time, assist Customer’s security personnel, and operate Supplier’s security solutions. To learn more on ERT Services see the **ERT Service Guide** abaliavle at: https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=bc348fe1-e90c-4e30-9d64-1d903006efa5.

“Negative Security Model” means that the service blocks requests from passing through only if they match a list of rules, and allows everything else to pass through.

“Onboarding Completion Milestone” means traffic redirection of >95% of the protected traffic from its origin to the applicable PoP, for at least one Protected Asset.

“Onboarding Process” means a process in which the Customer provides all needed parameters in order to provision and protect its Protected Assets. This process involves configurations both at the Service end and Customer end and is described in the **Cloud WAF Quick Start Guide** available at : https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=d320bfdc-0588-4025-9343-00dd931d3201

“**Point of Presence**” or “**PoP**” means a cloud-based data center facility operated by, or on behalf of, Supplier in order to deliver the Service.

“Positive Security Model” means that the service allows requests to pass through only if they match a list of rules, and blocks all other requests.

“**Protected Assets**” mean a set of Customer’s protected objects, network segments, servers or applications including but not limited to domain names, individual IP addresses and IP networks, which are protected by the Service and have been successfully onboarded to the Service through the completing of an Onboarding Process.

“**Scheduled Maintenance**” means any preventative, routine or scheduled maintenance that is performed on the Supplier’s facilities or any component used to deliver the Service thereof, (a) for which Supplier provides Customer notice at least 7 days in advance by email, or (b) recurring weekly maintenance window every Sunday between 7:00 AM EST and 9:00 AM EST. During this maintenance window the Service can be intermittently unavailable.

“**Service Level**” means each of the service level as described in Service Levels section of this CSS.

"Service Network Infrastructure" means the set of PoPs (and their specific internal components) that process customer's Protected Assets traffic to protect from attacks.

“Service Network Infrastructure Availability” means the proportion of time the Service Network Infrastructure is available, calculated annually.

“Service Portal” means the Service’s Customer facing Web application which provides data, reports and self-service capabilities relevant to the Protected Assets.

“Service Portal Availability” means the proportion of time the Service Portal is available, calculated annually.

North America

Radware Inc.

575 Corporate Drive

Mahwah, NJ 07430

Tel: +1-888-234-5763

International

Radware Ltd.

22 Raoul Wallenberg St.

Tel Aviv 69710, Israel

Tel: 972 3 766 8666