RADWARE TERMS AND CONDITIONS OF SALE (CLOUD SERVICES)

Unless specifically set forth otherwise in a signed agreement between you ("you" or "Purchaser") and Radware Ltd./ Radware Inc. ("Radware"), the following terms and conditions will apply to any sale/purchase transaction for Radware's cloud services. Radware is not bound by, and expressly rejects, any terms and conditions of your purchase order or any other offer or document, whether oral or written, which attempt to impose any conditions that are additional, conflicting or inconsistent with the following terms and conditions:

1. These Radware Terms and Conditions of Sales apply to any Radware cloud services purchased by you from time to time including any hardware and/or software provided by Radware in connection therewith (the "**Cloud Services**").
2. If you purchase a hardware or software product in connection with a Cloud Service – product warranty, DOA, RMA, end of life and maintenance and support services are provided pursuant to Radware's Certainty Support Guide as published by Radware from time to time at http://www.radware.com/Support/Certainty-Support-Program/ ("CSG"). If needed, username and password to access the CSG are available upon request. Exclusive remedies for failure of warranty are repair, replacement, reperformance of service or pro rata refund of purchase price.
3. EXCEPT AS EXPLICITYLY SET FORTH OTHERWISE IN THESE AGREED TERMS AND CONDITIONS OF SALE, THE ABOVE WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED AND EXCEPT FOR THE LIMITED WARRANTIES SET FORTH IN THESE TERMS AND CONDITIONS OF SALE OR MANDATORILY PROVIDED BY THE APPLICABLE LAW, RADWARE'S PRODUCTS AND ANY SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED.
4. The commencement date of a Cloud Service and any extensions, add-ons or renewals thereof will be three business days after the date of receipt by Radware of the purchase order for any such item. The duration of every Cloud Service and renewals thereof will be the duration set forth in the purchase order for same as confirmed by Radware. Cloud Service extensions and add-ons will expire together with the expiration of the Cloud Service to which they relate.
5. If your use of any Cloud Service exceeds the service plan purchased by you, you agree to pay for your excess use the upgrade fees as required under Radware's price list which has been provided or is otherwise available upon request. If you do not pay for your excess use of a Cloud Service that can be monitored by you or after being informed that you are in excess of your purchased service plan, Radware reserves the right to suspend your Cloud Service until full payment and eventually terminate these Terms and Conditions of Sale according to section 8 below.
6. All intellectual property rights embodied in the Cloud Services are exclusively owned by Radware.
7. These Terms and Condition of Sale shall be governed and construed in accordance with the substantive laws of, and venue will be located in: (i) Israel if Purchaser is located in Israel; (ii) England and Wales if Purchaser is located in EMEA; (iii) Singapore if Purchaser is located in APAC; and (iv) the state of New York for all other Purchaser locations.
8. If you or Radware materially breaches these Terms and Conditions of Sale and does not cure the breach within thirty (30) days after receipt of written notice of the breach, the non-breaching party may terminate these Terms and Conditions of Sale for cause immediately and without formal notice, but solely with regard to the sale/purchase transaction in connection with which the material breach shall have occurred.

9. **Neither you nor Radware shall be liable to the other 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 Cloud Services purchased by you, however caused, and whether based on contract, tort (including negligence), equity or other theory of liability whatsoever, even if advised of the possibility of such damages or losses or expenses. Without derogating from the foregoing, in no event shall the total aggregate liability of you or Radware to the other exceed the total aggregate fees received by Radware for the Cloud Services that are the subject matter of the liability in the 12 month period preceding the damaging event. This section will survive the termination/expiration of any sale/purchase document relating to the Cloud Services. The foregoing limitations will not apply with regard to damages arising from fraud or willful misconduct or any other mandatory exception under applicable law.**

10. Except for payment obligations, neither you nor Radware shall be liable to the other, nor be deemed to be in default under, or in breach of any provision of, these Terms and Conditions of Sale for the nonperformance or delay in performance of any of your or Radware's obligations (respectively) under these Terms and Conditions of Sale when such nonperformance or delay is due to Force Majeure Events. "Force Majeure Events" means: (i) acts of God, (ii) flood, fire, earthquake, tornado, tsunami, storm or explosion, (iii) war, invasion, riot, or other civil unrest, (iv) pandemics, epidemics, or quarantine restrictions, (v) government regulations or orders, (vi) action by any governmental authority, (vii) national or regional emergency, (viii) strikes, labor stoppages or slowdowns or other industrial disturbances, (ix) shortage of adequate power or transportation facilities, or (x) any other event which is beyond the reasonable control of you or Radware , as applicable. The party suffering a Force Majeure Event shall give notice of such Force Majeure Event as soon as reasonably practicable to the other party.
11. You are the controller of personal data transferred by you or by your customers to Radware and Radware is the data processor. Radware and Purchaser will each comply with its respective obligations as data processor/controller under applicable privacy & data security laws and, where applicable, pursuant to the Radware DPA available at https://www.radware.com/documents/dpa-customer/.
    You authorize Radware to engage other processors for carrying out processing activities on behalf of the Purchaser including the sub-processors listed at https://www.radware.com/documents/cloud-subprocessors/.
12. If one or more terms of these Terms and Conditions of Sale become or are declared to be illegal or otherwise unenforceable by any court of competent jurisdiction, each such part or term shall be null and void and shall be deemed deleted from this these Terms and Conditions of Sale. All remaining terms of these Terms and Conditions of Sale shall remain in full force and effect.
13. Your Cloud Service Schedule is attached.

Cloud DDoS Protection: Service Schedule

THIS CLOUD SERVICE SCHEDULE ("**CSS**") is sets forth Service-specific terms and conditions that govern orders placed by you directly or indirectly, through a reseller, channel or distributor (you shall be referred to as "Customer") for Radware Ltd./Inc.'s ("Supplier") **Cloud DDoS Protection Service** (the "**Service**").

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, 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.

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**
Time-to-Detect *per method*	Under Diversion	Sub-second	Sub-second	Sub-second	Sub-second
	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 Services Guide.

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.

"**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 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-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