Lumen Service Guide

Application Delivery Solutions Service Guide

Version: June 27, 2024

This Service Guide ("Service Guide") is subject to and incorporated into the Agreement and Application Delivery Solutions Service Schedule between the parties.

1. Application Delivery Solutions Features.

- Regional Egress supports regional egress data plans (includes requests to origin as egress).
- Core Platform is required with the Application Delivery Solutions – Regional Egress plan. It supports end user termination, Authoritative DNS, TLS, Geo-restriction and authentication.
- Custom Docker Container is an Application Delivery Solutions custom Docker Container that supports serverless functions. Container usage charges apply. License must be provided by Customer.
- OpenResty is a container supporting OpenResty NginX and LUA. OpenResty is open source software. Container usage charges apply.
- Varnish Cache is a container supporting Varnish Cache and VCL scripting. Varnish Cache is open source software. Container usage charges apply.
- Virtual Waiting Room (VWR) is a container supporting Virtual Waiting Room. Container usage charges apply.
- NodeJS is a container supporting the NodeJS protocol. NodeJS is open source software, and the container usage rate is priced on an Individual Case Basis (ICB).
- White Glove Support is Application Delivery Solutions White Glove Support performed by Lumen's vendor. Additional terms may be required.

The Application Delivery Solutions Aperture Portal is self-service enabled. If Customer activates and generates usage on a container or Node Type that does not have a negotiated rate on an executed Order, then the following rates will apply (rate per million requests [Mreq] per month). Rates are subject to change at any time.

Container Type	Rate
Varnish Cache	$0.64 / Mreq
OpenResty	$1.25 / Mreq
Virtual Waiting Room	$1.99 / Mreq
ThreatX	$0.98 / Mreq
Human Security	$0.63 / Mreq
Cloudinary	$0.63 / Mreq
Optidash	$0.63 / Mreq
SiteSpect	$1.99 / Mreq
Wallarm	$0.63 / Mreq
Radware	$0.63 / Mreq

2. Software Marketplace.

2.1 If Customer will use the Services to process personal data subject to data protection law that requires specific terms in place with the vendor or with Lumen (as applicable) as a processor, Customer agrees that it is Customer's sole responsibility to request the appropriate terms.

2.2 For any software designated as Third-Party Marketplace Software, Lumen offers quoting, ordering and billing support only. Third Party Marketplace Software is not part of the Application Delivery Solutions Services (as defined in the Schedule) provided by Lumen, and Customer acquires them directly from the applicable vendor or via a URL included within this Service Guide and Customer will be required to agree to the applicable vendor's then current standard terms and conditions as a condition of having access to the software via Lumen's Software Marketplace. Lumen is not responsible or liable for any damages whatsoever for Third Party Marketplace Software, even if Lumen recommends the software, or if the software is related to or complements the Service or to Customer's ability to use or receive the Application Delivery Solutions. Lumen is the applicable vendor's agent for purposes of ordering, collecting payment or in other ways as it relates to Third Party Marketplace Software.

Customer acknowledges that fees, payment, pricing, billing and tax terms are governed by the Agreement, Application Delivery Solutions Service Schedule, and the applicable Orders between Customer and Lumen. In addition, Lumen reserves the right to exercise all available remedies under the Agreement, including suspension for non-payment.

2.3 Customers may utilize their own license for certain software available on the Software Marketplace.

© Lumen Technologies. All Rights Reserved.

2.4 Customer consents to Lumen and the applicable vendors collecting and compiling system and operational metrics data to determine trends and improve service capabilities. Lumen and its vendors may associate this data with similar data of other Customers so long as such data is merged in a manner that will not in any way reveal the data as being attributable to any specific Customer.

3. Web Application Firewall (WAF) and BOT Management. All software is provided "AS-IS" and "AS-AVAILABLE" with no applicable service level agreement.

3.1 Customer may select one of the following self-managed WAF service features currently available and provided and licensed through Lumen: ThreatX or Wallarm.

3.2 Bot Management Services. Customer may select one of the following self-managed Bot, Account and Code defense features currently available and provided and licensed through Lumen: Human Security or Radware.

3.3 ThreatX, Wallarm, Human Security and Radware are software-as-a-service ("SaaS") services installed on a container. Applicable charges include implementation and technical supports costs.

3.4 Access and Monitoring. ThreatX is responsible for monitoring Customer WAF services, enabling application level monitoring and resolving potential security incidents. Customer will have access to the respective vendor's portal. Wallarm is responsible for monitoring Customer WAF services, enabling application level monitoring and resolving potential security incidents. Customers will have access to the respective vendor's portal.

3.5 Maintenance and Support. ThreatX is responsible for change management, major and minor releases, patch releases, service maintenance during vendor determined maintenance windows and all support during installation, service migration, Customer validation, and 24 x 7 monitoring and management after installation. Wallarm is responsible for change management, major and minor releases, patch releases, service maintenance during vendor determined maintenance windows and all support during installation, service migration, Customer validation, and 24 x 7 monitoring and management after installation.

4. Bot Risk Management (BRM). Customers may select Human Security or Radware for Bot Risk Management services. Human Security is designated Third Party Software and Services. Radware is provided through Lumen. Both Radware and Human Security are subject to the additional terms below. Unless otherwise expressly provided below, Bot Risk Management services are provided "AS-IS" and "AS-AVAILABLE" with no applicable service level agreement.

4.1 Human Security is a software module installed on an Application Delivery Solutions container supporting Human Security BotRisk Management. Container usage charges apply. Customer may provide its own Human Security license.

4.1.1 Human Security software is designated Third Party Marketplace Software and Customer agrees that its use of the software is subject to all of the terms, conditions, and requirements below. In addition, all terms of Section 2 above will apply.

> Customer's use of the software is subject to the Human Security Subscription Agreement found at https://www.humansecurity.com/subscription-agreement. All billing disputes must be made in writing within 20 days after the date of the invoice containing the amount in question to be eligible to receive an adjustment or credit. Any paid term will automatically renew unless either Human Security or the Customer provides the other with written notice of non-renewal at least 60 days prior to the renewal date. Software is provided as-is and as-available with no applicable SLA. Unless otherwise stated, all fees are in US Dollars.

4.1.2 All requests for licenses are subject to acceptance by Human Security. Delivery will be deemed to have been made when Human Security makes the Service available to Customer. Human Security will not provide Lumen with access to any Customer data related to or derived from Customer's use of the Human Security license.

4.1.3 Human Security may make changes to the SLA at any time upon at least sixty (60) days prior notice. Customer will make any request to Lumen for a credit under the applicable SLA. Lumen will credit a subsequent invoice for the amount of the applicable credit based on whether and to the extent Human Security agrees it is responsible for a failure under the SLA and agrees to provide a credit to Lumen. In no event will any credit exceed the amount of fees owed in the applicable month.

4.1.4 Human Security is responsible for providing support to Customer per the terms of the Subscription Agreement.

4.2 Radware offers a Bot Risk Management service. Radware software is installed on a container and is provided/licensed by Lumen subject to the additional terms below. This service is focused on mitigating bot attacks against Customer web services. Radware service makes real-time decisions to distinguish between activity of human visitors, activity of desirable automated software systems (i.e., good bots) and activity of malicious automated software systems (i.e., bad bots) so that controls can be put in place to limit automated and programmatic web and mobile application access. This service monitors incoming requests for validity, human visitors, or from good bots such as search engines, and not from automated software systems with malicious or undesirable intent. The service uses a number of

© Lumen Technologies. All Rights Reserved.

vendor proprietary techniques to detect automated software systems, including but not limited to unique, behavioral-based learning mechanisms that gather knowledge over time to detect and block malicious bots. With continued use, the Service's behavioral-based learning mechanisms learn, adapt and improve on its ability to detect the automated software systems attempting to access the Customer's web and mobile applications.

4.2.1 Use of Radware includes threat analysis capabilities that are deployed in the Docker containers and threat analysis capability that is deployed in the Radware cloud environment.

4.2.2 Radware is responsible for providing support to Customer per the terms of the Radware Terms of Service. The service fees are based on traffic volumes (monthly bot calls and the number of subscriber IDs). Additional support service are available as hourly service packages.

4.2.3 Customer's use of Radware Bot Risk management service is also subject to the "Radware Terms of Service", which means the terms and conditions incorporated as a binding attachment to the Service Schedule and available at https://www.radware.com/documents/eula-lumen/. Radware's Terms of Service also requires Customer's acceptance of the Radware DPA or "Data Processing Agreement" which means Radware's data processing agreement that forms an integral part of the Radware Terms of Service.

4.2.4 Lumen may increase rates on an annual basis.

4.2.5 Customer's Order is subject to acceptance of the corresponding order by Radware.

4.2.6 NOTWITHSTANDING ANYTHING TO THE CONTRARY, LUMEN'S AND ITS SUPPLIER'S AGGREGATE LIABILITY FOR DIRECT DAMAGES WILL BE LIMITED TO THE AGGREGATE AMOUNT RECEIVED BY SUPPLIER FOR THE SERVICE THAT IS THE SUBJECT MATTER OF THE LIABILITY IN THE TWELVE (12) MONTH PERIOD PRECEDING THE EVENT.

5. Image Optimization.

Cloudinary is a software module installed on a container supporting Cloudinary Image Optimization. The Cloudinary license must be provided by Customer.

Optidash Container is a software module installed on a container supporting Optidash Image Optimization. Customer agrees to the rates provided in the Order if Optidash is purchased by Customer and included within the container. Optidash is provided "AS-IS" and "AS-AVAILABLE" and no applicable service level agreement applies.

6. A/B Testing.

SiteSpect is a software module installed on an Application Delivery Solutions container supporting SiteSpect A/B Testing. Customer may provide its own SiteSpect license. If Customer purchases access to this software from Lumen, Customer will pay the minimum commit and applicable overages as provided in the order. The software is provided "AS-IS" and "AS-AVAILABLE" and no applicable service level agreement applies.

7. License Caps and Upgrades.

If the Customer exceeds the Service cap in a 2 consecutive month period, Service will be provided "as-is" and Customer will not be eligible for any Service Levels or Service Level credits that may otherwise apply until Customer takes the required action requested by Lumen as further provided herein. After any 2 consecutive month period, Lumen will provide Customer notice that it has exceeded the applicable service cap(s) and will request an upgrade of Service. If Customer either refuses to upgrade or does not respond to Lumen's request for an upgrade within 30 days of receipt of the notice, Lumen will automatically migrate Customer to the appropriate usage tier plan at standard rates. Lumen will deem Customer's refusal, inaction or failure to respond as its consent to migrate to the new plan for the remainder of the applicable term. Lumen may provide notice to Customer by sending a message to the email address then associated with the Customer account per Lumen's records. Notices provided by email will be effective when the email is sent. It is Customer's responsibility to keep its email address current. Customer will be deemed to have received any email sent to the email address then associated with the Customer account when the email is sent, whether or not Customer actually receives the email.

8. Pricing

8.1 Certain services may have fixed monthly recurring charges with overage charges based on traffic or other usage. If Customer exceeds the license size ordered on a regular basis (as determined by Lumen or the applicable vendor at its sole discretion), Lumen and/or the applicable vendor reserves the right to require a license upgrade.

8.2 Recurring ThreatX WAF or APS service pricing is based on number requests (HTTP/HTTPS) per month (i.e., committed traffic volume). Lumen captures this usage information from the Application Delivery Solutions platform or directly from ThreatX.

© Lumen Technologies. All Rights Reserved.

8.3 Recurring Wallarm WAF or APS pricing is based on number of requests (HTTP/HTTPS) per month (i.e., committed traffic volume). Lumen captures this information from the Application Delivery Solutions platform or directly from Wallarm.

8.3 Recurring Human Security Bot Defender and Account Defender pricing is based on number of requests (HTTP/HTTPS) per month (i.e., committed traffic volume). Code Defender pricing is based on unique visits per month (i.e. committed traffic volume). Lumen captures this information from the Application Delivery Solutions platform or directly from Human Security.

8.4 Recurring Radware Bot Manager pricing is based on number of requests (HTTP/HTTPS) per month (i.e., committed traffic volume). Lumen captures this information from the Application Delivery Solutions platform or directly from Radware.

9. Billing; Invoices.

The billing line item descriptions on the invoice will appear as DDoS Proxy Service instances with Attack Bandwidth and Clear Traffic Return numbers. These numbers map to Application Delivery Solutions licenses in the following manner:

Billing Description							
DDoS Proxy Instance							
			License Vendor				
Attack Bandwidth	10G	map to	ThreatX				
	20G	map to	Wallarm				
	30G	map to	Human				
	50G	map to	Radware				
	Unlimited	map to	ADS Platform				
			License Type				
			ThreatX	**Wallarm**	**Human Security**	**Radware**	**ADS Platform**
Clean Traffic Return Bandwidth	100	map to	WAF	Gold WAF	Bot Defender	Bot Manager	Platform
	250	map to	API	Platinum WAF	Code Defender	-	White Glove
	500	map to	-	API	Account Defender	-	-
	1000	map to	-	-	-	-	-
	2000	map to	Custom	Custom	Custom	Custom	Custom

10. Definitions.

"Web Application Firewall" or "WAF" means a service focused on protecting web applications from cyber-attacks by filtering, monitoring, analyzing, and blocking cyber threats. WAF is focused on HTTP traffic that web applications face. Web application attacks usually include cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection.

"Bot Risk Management" means a service that protects web applications against bad bot attacks. Bad bots represent software programs that malicious attackers use to automate their attacks.

"Workspace(s)" means each logical grouping of Customer's web applications which are managed and visible as a single grouping through the applicable Portal.