Lumen Service Guide

Distributed Denial of Service ("DDoS") Mitigation Service

Updated October 25, 2022

This Service Guide ("Service Guide") for DDoS Mitigation Services and related services and Application Protection Services is subject to and incorporated into the Agreement and Lumen DDoS Mitigation Services Service Schedule between the parties.

DDoS Mitigation Services.

The following features are additional add-ons available to Customer. All features may not be available for DDoS Hyper. Customer must either purchase the add-on or opt-in to receive it if it's a feature that isn't subject to an additional charge.

1. Direct Service. Direct Service is activated by BGP route advertisement, with logical private line connections over IPVPN between the Mitigation Infrastructure and Customer's border router(s). BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack.

For Direct Service, Customer must procure from Lumen connectivity between the Lumen network and the Customer premises or data centers (border routers) per the following criteria: (i) the demarcation point is the physical network port of the Mitigation Infrastructure, (ii) the connectivity must consist of at least one (1) IPVPN circuit directly to the port on the Mitigation Infrastructure from each of Customer's premises or data centers, and (iii) any Ethernet circuit must support 802.1Q. Provisioning begins upon confirmation of IPVPN circuit availability. Lumen may suspend Direct Services if Lumen detects that any Customer provided equipment is causing interference with the Lumen network or other customers. Any IPVPN circuit provided by Lumen will be subject to service levels as set forth in Lumen's standard service schedule for such service or as otherwise agreed in writing by Customer and Lumen.

2. Internet Direct Service. Internet Direct Service is activated by BGP route advertisement of the protected subnets with a specific community string attached (only applicable if Lumen Internet is currently configured with a public BGP peer) or Internet Direct Service can be configured as a static route (only applicable if the protected subnets are currently configured as a static route via Lumen Internet service) to deliver Mitigated traffic from the Mitigation Infrastructure to Customer's border router(s) via a shared VLAN that also delivers the Internet traffic or a separate VLAN on a Lumen provided Internet connection. BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack. Customer's routing equipment (if using BGP) should be configured to ignore route advertisements of protected subnets sourced from Lumen's Mitigation Infrastructure, which may be more specific and received from public internet routing tables. This is to prevent routing loops in which the Customer equipment may forward clean traffic from the Mitigation Infrastructure back out to the public Internet to be scrubbed again.

For Internet Direct Service, Customer must procure from Lumen connectivity between the Lumen network and the Customer premises or data centers (border routers) per the following criteria: (i) the demarcation point is the physical network port of the Mitigation Infrastructure, (ii) the connectivity must consist of at least one (1) Lumen Internet Service circuit capable of connecting to the port on the Mitigation Infrastructure from each of Customer's premises or data centers (subject to availability), and (iii) any Ethernet circuit must support 802.1Q for delivery of Internet and scrubbed traffic on a shared VLAN that also delivers the Internet traffic or two (2) separate VLANs. Provisioning begins upon confirmation of Lumen Internet Service circuit availability. Lumen may suspend Internet Direct Services if Lumen detects that any Customer provided equipment is causing interference with the Lumen network or other customers. Any Lumen Internet Service circuit provided by Lumen will be subject to service levels as set forth in Lumen's standard service schedule for such service or as otherwise agreed in writing by Customer and Lumen.

3. GRE Service. GRE Service is activated by BGP route advertisement and is based upon the GRE protocol with virtual tunnel connections constructed to Customer's border router(s). BGP routing protocol is used to communicate network advertisements from Customer to the Mitigation Infrastructure, enabling inbound traffic to route through the Mitigation Infrastructure during an Attack or threatened Attack. Customers directly connected to the Lumen AS IP network can advertise a /32 subnet for IPv4 or /128 subnet for IPv6. Non-Lumen IP customers must advertise a /24 subnet for IPv4 and a /48 subnet for IPv6 as a minimum.

4. Routing under either the Direct Service, Internet Direct Service, or the GRE Service is asymmetric, with outgoing traffic from Customer to the Internet being forwarded as normal to Customer's Internet service provider, without passing through Mitigation Infrastructure.

5. Monitoring. Monitoring options for the DDoS Service are designed to provide proactive detection of DDoS Events ("Attack Monitoring Services"). Attack Monitoring Services are available as described below:

(a) Flow Based Monitoring ("FBM") provides 24x7 monitoring and alerts for large flood-based Attacks: (1) from Customer owned and managed equipment; or (2) from Lumen provided and managed equipment installed on Customer's premise, or (3) with Lumen

Internet Services that choose monitoring from Lumen provider edge routers. FBM Service requires a reliable feed of netflow sampling and SNMP specific to the Customer's traffic. To the extent Customer purchases the FBM Service with the On-Demand Service, Lumen will proactively notify Customer about DDoS Mitigation system generated alarms that Lumen detects are caused by DDoS Attacks. For Attacks that are not detected by the DDoS Mtigation system, Customer must contact the SOC to initiate Mitigation. For option 1 and 2 above, there will be an MRC and an NRC for each piece of equipment when monitoring occurs from the Customer premise. For option 3 above, an MRC and an NRC for each logical circuit when monitoring occurs from Lumen provider edge routers directly from which the FBM Service collects netflow sampling.

If Customer purchases FBM and also procures from Lumen Internet connectivity and Lumen is the only provider who provides Customer Internet connectivity, Customer has the option to pre-authorize Lumen to configure systems to automatically initiate Mitigation for each attack detected by FBM. If Customer selects the auto-mitigate option, Customer must provide Lumen written notice via a change ticket in Control Center of its pre-authorized permission to begin Mitigation. Customer may later withdraw pre-authorized permission via a change ticket. Change tickets require 24 hours advance notice.

(b) Application Monitoring and Mitigation ("AMM Cloud Signaling") is hardware based DDoS detection and Mitigation, requiring Customer provided hardware and embedded operating software at the Customer premise ("Customer CPE") to monitor the Customer's perimeter network traffic and issues alerts for layer 7 or "application layer" Attacks. Customer must be able to provide Cloud Signaling from Customer CPE to Lumen's Cloud Signaling endpoint and Customer is responsible for technical support, service and maintenance of the Customer CPE. Customer will have full administrative access to the Customer CPE and Lumen will have no access to the Customer CPE. There will be an MRC and an NRC for each Customer CPE utilizing the AMM Cloud Signaling Service.

Notwithstanding the foregoing, Lumen reserves the right at any time to: (i) change or supplement the monitoring tools and the Mitigation techniques (including but not limited to modifying the Mitigation Infrastructure); (ii) increase or decrease the monitoring tools' sensitivity to anomalous IP traffic patterns; and (iii) modify the definition of anomalous IP traffic patterns that may indicate an Attack.

6. SOC Advanced Support is an optional add-on feature that includes a quantity of hours per month, to be identified in the Order or within DDoS Hyper, of consulting, advisory and operational services by providing a designated, remote point of contact for the Customer throughout the term of the DDoS Mitigation Service. A Lumen Security Specialist will perform a variety of support tasks, as well as ongoing support and consultative activities related to the Lumen DDoS Mitigation service.

SOC Advanced Support, which may also be referred to as Professional Security Service Assistance or PSSA, is performed remotely by English speaking Lumen personnel (e.g. Lumen employees or contractors) located in the United States between the hours of 9:00 A.M. and 5:00 P.M. local time within the continental United States, Monday through Friday, and excluding United Sates statutory holidays and any additional holidays that Lumen grants to its employees, a list of which can be provided to Customer prior to the commencement of the Services upon request. If Customer requests SOC Advanced Support outside of such hours (non-standard hours), Customer will be responsible for any additional costs incurred as a result, as may be legally required (including without limitation any overtime pay). Lumen will determine the personnel assigned to perform the Service. No SLA applies to SOC Advanced Support Services.

(a) Performance of Services by Lumen personnel is not intended to modify or change the status of such resource to that of any employee of Customer.

(b) The specific services that are desired by the Customer from the list attached as Exhibit A to this Service Guide will be determined and mutually agreed upon during the kick-off call. Commencement of billing for SOC Advanced Support is concurrent with the Service Commencement Date for DDoS Services.

(c) Customer agrees to complete an upfront questionnaire that gathers necessary context for performance of the SOC Advanced Support Services including but not limited to: (i) Business context being protected by DDoS Service; (ii) Identify any applicable compliance standards that apply to their business; (iii) Identify any existing DDoS concerns; (iv) identify any business changes that may have near-term impacts on traffic patterns impacting DDoS protection. In addition, Customer agrees to (i) provide a point of contact to coordinate the service activities; (ii) provide Lumen with timely responses to inquiries around providing the service; (iii) timely participation in phone call(s) to discuss conditions or questions regarding any activities; (iv) specifically identify and provide Lumen with access to all relevant Customer-controlled information, resources and locations required to perform and/or complete the Services.

7. Rapid Threat Defense. Rapid Threat Defense is an automated threat detection and response capability designed to detect and block bots based on identified behavior and confidence by Lumen's proprietary research labs ("Black Lotus Labs"). When bots are discovered that meet or exceed the confidence level, these identified bots are automatically deployed to the DDoS Mitigation Service to be used as countermeasures during an active DDoS Attack. Due to the varying nature of malicious activity, Lumen cannot guarantee that all malicious activities intended to be blocked will be identified, detected and blocked. Customer can view automated actions via DDoS Mitigation Service Portal.

Application Protection Services.

1. Application Security Services Features. Application Security Services may also be referred to as Web Application and API Protections, WAF services and/or Web Application Firewall services. All software is Software as a Service (SaaS) and made available

to Customer via the Customer's pre-established and credentialed connection to the applicable vendor portal. Currently supported software is listed below and further described below:

ThreatX WAF Software as a service (SaaS) with API protection and bot management
Wallarm WAF SaaS with API protection and bot management
PerimeterX SaaS bot management
Radware SaaS bot management

2. Third Party Software. 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.

3. Web Application Firewall (WAF). Customer may select one of the following managed WAF service features currently available and provided and licensed through Lumen: ThreatX or Wallarm. WAF software is provided "AS-IS" and "AS-AVAILABLE" with no applicable service level agreement.

3.1 Wallarm Cloud WAF allows Customers to build cloud-native applications securely, monitor them for modern threats, and get alerted when threats arise. Wallarm Cloud Web Application and API Protection (WAAP) includes full support of API technologies including REST, SOAP, WebSocket, graphQL and gRPC.

3.2 Pricing and Billing.

3.2.1 ThreatX WAF service pricing is based on two pricing models, both billed as a monthly recurring charge: (1) number of supported applications or domain groups (small, medium, large, jumbo) and number of requests (HTTP/HTTPS) per month (i.e., committed traffic volume) or (2) number of requests (HTTP/HTTPS) per month only (small, medium, large, extra-large (XL), XL1, XL2, XL3, XL4, XL5, XL6, XL7, XL8. Lumen captures this usage information directly from ThreatX on a monthly basis. Lumen will notify Customer when Customer's actual traffic volume (i.e., committed maximum traffic or maximum number of requests, as applicable) exceeds the contracted committed traffic or number of requests for two (2) consecutive calendar months. If Customer does not respond and agree to an upgrade to a higher subscriber/license tier within 30 calendar days, Lumen will not be responsible for the effectiveness of the WAF service beyond the contractually committed volume nor will Lumen be liable for any failure to provide Service. Customer's failure to upgrade Services and Lumen's provision of Service thereafter on an "as-is" "as-available basis" is not a basis for Customer's ability to terminate the Services for default or deficiency in Service. Lumen's failure to notify Customer of traffic overages at any time will not be deemed to limit Lumen's right to notify Customer and require a subscription upgrade for any subsequent instances of traffic overages.

3.2.2 Wallarm WAF pricing is a monthly recurring charge based on number of requests (HTTP/HTTPS) per month (i.e., committed traffic volume). Lumen captures this information directly from Wallarm.

3.3 Access and Monitoring. ThreatX endeavors to monitor Customer's WAF services, enable application level monitoring, identify and block potential security incidents**.** Wallarm endeavors to monitor Customer WAF services, enable application level monitoring, identify and block potential security incidents. Customers will have access to the respective vendor's portal.

3.4 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 Management. Customers may select PerimeterX or Radware for Bot Management services. PerimeterX is designated Third Party Software or Services. Radware is provided through Lumen, both subject to the additional terms below. Bot Management services are provided "AS-IS" and "AS-AVAILABLE" with no applicable service level agreement.

4.1 PerimeterX 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 and in the Service Schedule.

Customer's use of the software is subject to the PerimeterX Subscription Agreement found at www.PerimeterX.com/Legal/PSA.pdf. 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 PerimeterX or the Customer provides the other with written notice of non-renewal at least 60 days prior to the renewal date. Unless otherwise stated, all fees are in US Dollars.

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

4.1.2 The SLA applicable to the Services is found out www.PerimeterX.com/legal/SLA.pdf. Customer is responsible for coordinating directly with PerimeterX for SLA issues and credit. PerimeterX may make changes to the SLA at any time upon at least sixty (60) days prior notice. Customer will make any request to PerimeterX 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 PerimeterX 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.

4.1.3 PerimeterX is responsible for providing support to Customer per the terms of the Subscription Agreement.

4.2 Radware offers a Bot Management service. Radware 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 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 learns, adapts and improves 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 and threat analysis capability that are 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 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.

5. Definitions.

"Bot 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.

"Clean (Post-Mitigation) Traffic Capacity" means the level of traffic using standard DDoS Mitigation Service as identified on the Order that is returned to the Customer "clean" following the Mitigation process.

"Cloud Signaling" means the process by which Application Monitoring and Mitigation Serviceutilizes automated monitoring tools to detect anomalies in IP traffic patterns and signals a potential Attack to Lumen's Mitigation Infrastructure.

"Customer Disaster Recovery Site" ("DR Site") means an alternative backup site that is used when a primary location becomes unusable due to failure or disaster. Customer will not use the DDoS Mitigation Service with production traffic at the DR Site except when use of the Customer primary site fails.

"Customer-Initiated Mitigation" is an optional feature for Always-On DDoS Mitigation Direct Service, Internet Direct Service or GRE Service that allows customers to initiate mitigation via BGP route announcements to Lumen rather than calling the Lumen Security Operations Center ("SOC"). Customer-Initiated Mitigation is equivalent to Customer approval to route traffic to the Mitigation Infrastructure for purposes of the TTM SLA. Customer-Initiated Mitigation is subject to Lumen availability based on its network configuration. If available, Customer must dynamically advertise the preferred prefixes into the clean return tunnels and the advertised prefixes automatically propagate from the Mitigation Infrastructure to the Internet and the Service automatically begins scrubbing the advertised traffic. The maximum number of prefixes that can be advertised via Customer-Initiated Mitigation is subject to technical constraints. Customer may elect this feature at the time of provisioning or after the Service is turned up via a ticket or by submitting to the SOC.

"DDoS Mitigation GRE Service" or "GRE Service" means DDoS Mitigation implemented using BGP route advertisements as a mechanism to re-route legitimate and Attack traffic through the Mitigation Infrastructure. Clean traffic is routed back to the Customer data center using a GRE tunnel.

“DDoS Mitigation Direct Service” or “Direct Service” or “IP VPN Direct Service” means DDoS Mitigation implemented using BGP route advertisements as a mechanism to re-route legitimate and Attack traffic through the Mitigation Infrastructure. Clean traffic is routed back to the Customer data center over IPVPN/EVPL logical connections between the Mitigation Infrastructure and Customer’s border router(s).

“DDoS Mitigation Internet Direct Service” or “Internet Direct Service” means DDoS Mitigation implemented using BGP route advertisements as a mechanism to re-route legitimate and Attack traffic through the Mitigation Infrastructure. Clean traffic is delivered on a Lumen provided Internet Service circuit only back to the Customer data center over a shared VLAN logical connection that also delivers the Internet traffic or separate VLAN logical connection.

“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/HTTPS traffic that web applications face. Web application attacks usually include cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection.

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

EXHIBIT A
SOC Advanced Support

A list of SOC Advanced Support currently available are identified below. Lumen reserves the right to update the list of available services from time to time.

Advanced Onboarding and Activation with a Dedicated Security Engineer are available and charged at the rate identified in the Order and/or buy down the bucket of monthly hours purchased by Customer in lieu of standard onboarding services provided.

- Provide prompt activation support in emergency cases or scheduled activation support in non-emergency cases.
- Complete tuning session with Customer to confirm correct thresholds and protection types.
    - If an existing Lumen Customer, leverage tools to assist in identifying what Mitigation countermeasures would be initially used.
    - Customer historic DDoS activity reviews to help identify optimal policy threshold settings for alerts and Mitigation countermeasures; based on Customer feedback.
- Provide Customer onboarding and Service review.
    - Provide SOC runbook to Customer, containing SOC escalation and engagement process and overview of the Service
    - Portal training specifically for DDoS.
    - Verification that all required circuits are being protected.
    - Reviews and policy verifications for protected IPs and networks.
    - Mitigation alert policy review to verify appropriate contacts are notified.
    - Auto-mitigation versus manual Mitigation scenario reviews with Customer.
    - Regular automated reporting (monthly/quarterly as needed) within the Portal as requested by Customer.
        - Alerts
        - Mitigations
        - Traffic summary
- Liase with the Customer and Account Team for successful onboarding.
- Liase with other Lumen support groups as needed.

Additional SOC Advanced Support:

- Activation, testing, and tuning of the Customers DDOS services.
    - Review example configurations for GRE and CPE FBM with Customer and answer questions related to our requirements.
- Customer may request participation to monitor for potential attacks and assist as needed.
- Regular Service review

Monitoring and Configuration Analysis:

- DDoS Incident reviews for trending including targets, methods, and frequency.
- Mitigation zone grouping reviews with Customer for maximum Mitigation effectiveness.
- DDoS Mitigation Service separation reviews regarding customer's traffic and applications such as web, email and DNS.
- Configuration improvement reviews and recommendations for optimal protection.
- False positive reviews and recommended methods to limit future occurrences.

Regular (quarterly, semi-annual, or annual) DDoS Service Reporting:

- Reporting containing analysis, advice and recommendations.
    - DDoS Attack trending summary reports.
    - SOC ticket report generation and reviews with Customer with ongoing feedback provided to SOC.
- Regular reviews with Customer to discuss findings and recommendations.
    - Advisement of any new or additional IPs or networks that should be protected.
    - Advisement of recommended changes to DDoS Mitigation settings for optimal defense against Attacks.
    - Mitigation countermeasure tuning recommendations to prevent impacts to production environments and minimize false positives.
- Custom runbook updates based on Customer's needs.

Items not supported by SOC Advanced Support:

- Direct configuration of Customer routers or equipment.
- Advise on what configuration specifically to be inserted into Customer router or equipment.
- Custom reporting.
- Non-standard build requirements