# Kyndryl Edge Delivery Services – Service Descriptions

The following Service Descriptions are applicable to the purchase and use of various Kyndryl Edge Delivery Services and are incorporated into the Statement of Work (SOW) between Customer and Kyndryl. Kyndryl reserves the right to modify the Services Descriptions at any time. Kyndryl will provide prior notice via the Customer Portal or other electronic means for any Services that are being modified. Capitalized terms used but not defined herein will have the meanings set forth in the Agreement

**Table of Contents**



## GLOSSARY

**95/5**: The billing and measurement methodology shorthand describing a process of determining the 95th percentile of usage or the uncompressed equivalent as measured by Kyndryl over five minute intervals. The 95/5 methodology is used to measure usage of Services billed in Concurrent Users, GB Stored, Mbps, Gbps or any other bit per second methodology.

**95th Percentile Method:** means the process of i) measuring actual Content delivery in Mbps and/or NetStorage usage in GB at five (5) minute intervals throughout the month; ii) ranking such measurements from largest to smallest; iii) discarding the largest five percent (5%) of such measurements; and iv) calculating charges based on the measurement at the 95th percentile for the month.

**ACL**: Access Control List

**Edge Delivery University**: Instructor-led training courses, either web-based or located at an EDS training facility.

**Always-On**: Always-On refers to a service plan that provides traffic redirection through the Prolexic network at all times consistent with the applicable SLA for the service.

**Anonymous Users**: Users whose personal data and credentials are not captured and retained in the AIC.

**API**: Application Programming Interface

**Application (or App)**: Any discrete instance of computer software that performs a particular function for a Customer or Customer's end user and can be accelerated by any EDS acceleration Service. For billing purposes, each instance of any such software is considered an independent "Internet Application" or "App". For example, each Application running on a particular platform (e.g., Force.com, Amazon AWS, Microsoft Azure, SAP, .NET, etc.) is considered a discrete App, while the platform itself would not be considered an App. Also, a portal consisting of many Applications will be counted as more than one application.

**Beacon:** any HTTP request initiated by Customer's end user from the mPulse JavaScript that contains payload data.

**Business Day**: Monday through Friday for all regions excluding local, government-sanctioned holidays:

- North America (GMT-5:00): 9:00 AM to 9:00 PM ET
- Europe (CET): 9:00 AM to 6:00 PM
- Asia-India (GMT +05:30): 9:00 AM to 6:00 PM
- Asia-Japan/Singapore (GMT +8:00): 9:00 AM to 6:00 PM

**Change Request:** A Change Request is a customer driven request for Professional Services to complete a product configuration change to the Customers EDS production configuration. Changes are limited to those possible through existing Customer interfaces for EDS Services including the EDS portal, Property Manager, Certificate Provisioning System interface.

**CIR:** Committed information rate measured in megabits per second (Mbps).

**Clean Bandwidth**: Clean Bandwidth will be calculated on a monthly basis using the 95th percentile calculation and compared to the contractual CIR, with overage billing applied for exceeding the CIR. To compute the 95th

percentile value, EDS shall gather samples of clean traffic routed through the Prolexic Network and returned to the Protected Network or passed from the Protected Network, post-mitigation.
These samples will be collected at regular intervals. Kyndryl shall discard the highest 5% of the samples for each of inbound and outbound traffic, and the next highest sample becomes the 95th percentile value for the data set.

**Committed Information Rate for Prolexic Services**: CIR is the maximum rate of Clean Bandwidth that Customer may pass through the EDS scrubbing centers as detailed on the Order Form. The CIR should be selected such that the Customer's 95$^{th}$ percentile traffic should not normally exceed the contracted CIR, and such that the peak traffic does not exceed twice (2X) the contracted CIR.

**Content**: Information, software, and data that Customer provides, including, without limitation, any hypertext markup language files, scripts, programs, recordings, sound, music, graphics, images, applets or servlets that Customer or its subcontractors or Services recipients create, install, upload or transfer to or through the Edge Platform.

**CP Code**: Content provider code used to track Customer's individual usage of the applicable Service(s).

**Customer Contacts**: The set of contacts specified by Customer as the persons with whom Kyndryl should communicate regarding Service-related matters.

**Customer Insights:** Customer Insights is a cloud-based data analytics portal where Customers can view event and user profile information associated with their Identity Cloud subscription.

**Customer Portal:** Upon execution of the initial Transaction Document, Customer shall be provided access to the Customer Portal where a variety of billing, reporting and SLA information is available. Failure to meet the following requirements may result in undetected and/or unauthorized access. (a) Customer Portal user accounts should not be shared between individuals. (b) Setting responsible standards for passwords, including using unique passwords for each Customer Portal user account. Passwords used for the Customer Portal should not be shared with any other Kyndryl Edge Service. (c) Sufficient auditing of Customer portal user account(s), and user account activities, including removal of privileges and/or deactivation of accounts when associated employees leave the Customer's organization or transition to roles no longer requiring access to the customer portal

**Customer Team**: The discrete Customer contacts from an individual Customer corporate unit (e.g., legal entity, company business unit, publishing group, product brand, or application team) who are authorized on behalf of the Customer to consume EDS Service and Support. While a Customer Team may operate in multiple time zones, a single time zone must be declared with the purpose of establishing Customer Business Hours.

**Customer Business Hours**: Refers to 9:00 am to 5:00 pm (in the local time zone for the Customer Team) on Monday through Friday, excluding local holidays as defined by government sanctioned holidays.

**CVR**: Committed volume rate measured in gigabytes (GB) or terabytes (TB) transferred per month (or annually if so specified). For purposes of measurement and reporting one (1) TB equals one thousand (1,000) GB and one (1) GB equals one thousand (1,000) megabytes (MB).

**CVS:** Committed volume of storage measured in gigabytes (GB) used.

**DDoS (distributed denial-of-service) or DoS (denial-of-service) Attack**: An ongoing traffic increase where (i) Site traffic is four or more times higher than the average Site traffic, per unit, over the immediately preceding two month period, (ii) Customer and Kyndryl mutually agree that the traffic spike is malicious, and/or unwanted, and Customer requests Kyndryl to declare the traffic as a DDoS Attack, and (iii) Customer informs Kyndryl that they are willing to NOT serve the unexpected traffic and are willing to allow Kyndryl to determine the approach for mitigating potential negative impacts of the DDoS traffic (e.g., blocking the traffic, redirecting the traffic, serving the traffic, etc.).

**Domain**: An Internet domain name that comprises a string of typographic characters used to describe a specific online location associated with a web resource controlled by a discrete and individual corporate unit (e.g., a legal entity, company business unit, publishing group, product brand, or application). For example, in the case of *www.sample.com* and *images.customer.com*, "*sample.com*" and "*customer.com*" are the Domains whereas "*www*" and "*images*" are hostnames or sub domains included with the "*sample.com*" Domain and "*customer.com*" Domain, respectively. If a Customer controls a top-level domain, all strings consisting of a second-level domain followed by the top-level domain shall be considered part of the same Domain.

**EdgeScape Database**: EDS' proprietary database, and all information included therein, used to provide Site content providers with the Identification Code for assigned, route-able addresses in the commercial IP space.

**EDS:** Edge Delivery Services

**Feature Release** (or **Upgrade)**: A new release of Software that provides incremental and enhanced functionality over previous Software Releases.

**GB:** gigabyte(s). One (1) GB is equal to 1,000 MB.

**Gbps: g**igabit(s) per second. One (1) Gbps is equal to 1,000 Mbps.

**Generic Routing Encapsulation (GRE)**: refers to a tunneling protocol defined in IETF RFCs 1701 and 2784.

**GTM Datacenter**: A GTM Datacenter represents a co-located set of servers to which GTM will route Customer traffic.

**GTM Domain**: A GTM Domain is a grouping of GTM Properties. The type of domain determines the type of properties that can be created inside that domain. The available domain types depend on whether Customer has purchased GTM Standard or GTM Premier. Additionally, permissions on the EDS customer portal are set at the domain level.

**GTM Property**: A GTM Property is a set of IP addresses or CNAMEs that GTM provides in response to DNS queries based on a set of rules. The GTM rules to be applied depend on whether Customer has purchased GTM Standard or GTM Premier.

**Hardware Manufacturer**: The third party manufacturer of Aura Hardware.

**Hit:** a HTTP request to an Edge Platform server to access an object.

**Identification Code**: The information provided by the EdgeScape Database for each Site request, including, but not limited to identifying the geographic and network point-of-origin of such request.

**Identity**: An Identity is any entity (person, device, thing, etc.) that interacts with the customer application and Identity Cloud solution.

**Local Support Business Hours**: Local Support Business Hours are defined by Primary Major Geography during Business Days.

**Maintenance Update** (or **Update)**: A new Software release following the initial shipment of a Feature Release which rolls up fixes for known Software defects to the extent such release is made generally available by Kyndryl.

**Monthly Active Users:** The subset of Anonymous Users or Registered Users that have interacted with the Edge Identity Cloud application in any way during a calendar month.

**On-Demand**: On-Demand refers to a service that provides Customer with the ability to redirect traffic through Prolexic scrubbing centers on an as-needed basis, subject to Customer restoring normal traffic routes within 72 hours after the completion of a DDoS attack. Further, once such On-Demand services are engaged, if an identifiable attack is not detected by Kyndryl within 24 hours then Customer shall disengage and redirect traffic over normal routes.

**Order Form:** Also known as PCR or SOW**,** refers to process for communicating and documenting a change to the scope of the Services purchased.

**PCR:** Project Change Request

**Premium Reactive Support**: Technical support provided in response to Customer's Support Requests. Premium Reactive Support Service Includes:

- Premium Reactive Support for one Customer Team with Service coverage for one Primary Major Geography
- Prioritized Routing to senior support technology specialists
- Named Technical Support Engineer – during Customer Business hours—as available
- Unlimited Support Requests
- Premium Live Support Availability:
    - Live 24x7X365 support for S1 and/or S2 issues
    - Live support during Local Support Business hours for S3 issues
- Premium Support Service Level Agreement
    - Premium Initial Response Times
        - 30 minutes or less for S1 issues (must be opened via phone)
        - 1 hour or less for S2 issues
        - One Business Day for S3 issues

        - All Support Requests reported via e-mail will be considered as S3
    - Premium case status updates--Hourly for S1 issues. Less frequent updates may be provided when mutually agreed by Customer and Kyndryl.
- Premium Support Customer Engagement Guide ○ Communication, escalation, maintenance, and change management processes all following a custom operations support guide.

**Primary Major Geography**: Support operates in the following Primary Major Geographies: Americas, Europe, Asia – India, and Asia – Japan.

**Proactive Service Availability Monitoring**: Ongoing service to uncover potential, availability and configuration risks. Kyndryl proactively monitors issues on the EDS network that may affect availability of web and streaming content. Proactive Service Availability Monitoring keeps Customer informed of issues and provides recommendations for addressing them, but it does not include monitoring for website/application performance or EDS security Services. Proactive Service Availability Monitoring is available with Premium Support Services.

**Product Support**: The provision of telephone or web-based technical assistance by Kyndryl to Customer's technical contacts with respect to errors related to the corresponding products and features licensed for use on the EDS network by the Customer. The available variants of Product Support are: Standard Support, Named Enhanced Support, Enhanced Support SLA and Premium Support. Product Support is provided in accordance with the service descriptions defined herein. Product Support does not include assistance related to errors encountered under the use of EDS products for any purpose not stated in the service description or features of the supported products licensed by the Customer.

**Product Support for EDS Cloud Security Services**: This support is provided in accordance with the service descriptions and service levels specified in the Services Page under each of the Support Service levels (Standard Support, Priority Support, Enhanced Support SLA & Premium Support). Product Support for EDS cloud security Services includes:

- Support for product Errors encountered by the Customer
- Initial response and acknowledgement of Security Events identified and reported to technical support resources by Customer
- Verification that a Security Event is indeed the result of a third party attack that is taking place
- Customer is responsible for making changes to its Kona configuration via available mechanisms
- Customer assistance related to solving customer problems with basic use of Kona Services for Remedial Mitigation of the known active attack vectors via portal
- Technical support assistance and initial instruction is limited to up to:
    - 2 hours per Security Event for Customers with Standard Support, Priority Support, or Enhanced Support SLA - no more than 25 hours total in any given year.
    - 6 hours per Security Event for Customers with Premium Support - no more than 150 hours total in any given year.
- For assistance beyond these limits, Professional Services must be engaged at additional cost.

Product Support for Cloud Security Services does not include ongoing monitoring of Security Monitor or alerts by Kyndryl, monitoring of Customer bridge calls by Kyndryl, or the Professional Services required to identify or assess attack vectors, conduct attack response planning, provide Configuration Assistance, or custom rule development.

**Professional Services**: Professional Services, including integration services, is the term used to generally encompass the Services described under the Professional Service-related entries of the EDS Services Page. Notwithstanding any language to the contrary, Professional Services provided universe-wide shall be considered "North American Services" if such term is included in the Customer's Agreement. Professional Services are provided via phone, email and/or web conferencing at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).

**Protected Network**: Protected Network refers to the set of protected objects ingress and egress termination points including but not limited to domain names, individual IP addresses, protected subnets, IP networks, Customer border routers, and application services as enumerated in the Customer's Agreement.

**Protection Policy**: A Protection Policy is any combination of security controls deployed to the EDS network, which, depending on the features of the solution being purchased, may include "Slow POST" protection, rate

controls, reputation controls, network layer controls, and application layer controls. Customer's Protection Policy entitlement will be based on how many concurrent policies Customer has purchased.

**Registered Users**: Users whose personal data is captured and retained in AIC.

**Request:** A request to an Edge Platform server to retrieve an item of anonymous non-personally identifiable user data from an Edge Platform proprietary database or to perform a certain function based upon one or more Segments specified by Customer

**Remedial Mitigation**: The use of any standard mitigation tactic against known attack vectors**.**

**Security Event**: Any event causing suspicion of an actual or anticipated application level or denial of service attack.

**Security Incident**: A Security Event that has been reasonably confirmed by Kyndryl technical support resources to be an actual attack against a Customer's digital property, i.e., a Site requiring separately configured and distinct Application Services deployed on the Edge Platform, reporting feeds, or invoicing.

**Services Recipients:** Any entities or individuals receiving or using the Services (other than Customer), or the results or products of the Services.

**Severity Level**: The following is a guide for assigning appropriate severity levels for Support Requests:

| Severity Level | Impact | Description |
|---|---|---|
| Severity 1 (S1) | Critical | Service is significantly impaired and unavailable to multiple user locations, e.g., multiple Sites are affected. |
| Severity 2 (S2) | Major | Repeatable inability to use the applicable Service from a single location or region, e.g., localized Service outage issue. This might be to a single Site or even a single server. |
| Severity 3 (S3) | Low | Non-urgent matters or information requests, like planned configuration change requests, information requests, reports or usage questions, clarifications of documentation, or any feature enhancement suggestions. |

**Severity Level (Cloud Security Services)**: The following is a guide for assigning appropriate severity levels for Product Support for Cloud Security Services. Security analysts will perform an analysis of a Security Event. Whether a Security Event is considered a Security Incident is determined solely by Kyndryl. Identified events will be classified, prioritized, and escalated as Kyndryl deems appropriate. Security Incidents are classified into one of the three severity levels described below. These definitions below replace the Severity Level definitions above and apply specifically to EDS's Cloud Security Services.

| Severity Level | Impact | Description |
|---|---|---|
| Severity 1 (S1) | Critical | This class exhibits: a) loss or outage on any portion of a protected property, b) data breach (exfiltration or infiltration) confirmed in progress, or c) defacement of a protected property. |
| Severity 2 (S2) | Major | This class exhibits: a) degradation in performance on any portion of a protected property, b) suspected data breach, or c) excessive bot activity that may lead to intellectual property compromise. |
| Severity 3 (S3) | Low | This class exhibits: a) signs of a potential small-scale security incident (log event evidence of malicious traffic that does not impact the origin and may be false positive), b) is a proactive action; "heightened attention" in response to a public threat, for instance, c) includes a possible fraud investigation without immediate evidence of data breach, or d) low-level site scraping activity. |

**Site**: A set of URLs used to deliver content and Applications for a discrete and individual corporate unit (e.g., legal entity, company business unit, publishing group, product brand, or Application) that may consist of at most one domain and up to 10 hostnames. For example, in the case of www.customer.com and images.customer.com "customer.com" is the domain and "www" and "images" are hostnames.

**Software Release**: A Feature Release and/or Maintenance Update, as applicable.

**Strict IP Whitelist**: A configuration option within the Kona Web Application Firewall network-layer controls in which requests are processed solely for the IP addresses within the IP Whitelist, whereas requests from all other IP addresses are explicitly denied a connection to an EDS edge server.

**SSL:** secure sockets layer

**SSL Network Access**: A network resource allocated to Customer for the purpose of accelerating SSL sessions with a X.509 digital certificate. Customer purchases the type of digital certificate to be included with the SSL Network Access, such as Standard (Single-Hostname), Wildcard, SAN, Extended Validation (EV), Extended Validation SAN or Third Party.

**Subcontractor:** A contractor, vendor, agent, or consultant selected and retained by Kyndryl or Customer, respectively.

**Support Advocacy**: Support Advocacy is provided by a named contact (i.e., a Support Advocate) that works with the Customer Team to support Customer's success by providing enhanced, personalized, proactive support services during Customer Business Hours. The Support Advocate will help plan, manage, and direct ongoing Support engagements to ensure that Customer achieves maximum value from EDS Services. The Support Advocate will develop a custom support engagement guide including deliverables focused in the following areas:

- **Premium support package fulfillment ownership**
  - Customer Support onboarding
  - Monitor open case progress
  - NPS/CSAT survey follow-up
  - Customer touch point meetings
  - Drive continuous Support improvement
- **Support Champion**
  - Single point of Support escalation
  - Facilitates & lead resolution of complex problems
  - Represents Support as a member of the internal account team
  - Active participation at Quarterly Business Reviews/Quarterly Service Reviews and monthly compliance/cadence reports
- **Proactive Support**
  - Drive problem prevention
  - Identify areas of improvement
    - Training
    - Optimize and customize availability alerting.
- **Upgrades, Changes and Customer Events**
  - Participate in Customer planning & implementation sessions.
  - Configure relevant alerts
  - Drive event awareness with support team
  - Follow up on all cases from the event (analysis and summary)

**Support Requests**: Service support calls or online support tickets initiated by Customer where the underlying issue is determined to reside in Customer's host environment (not in the EDS Services or EDS network) or other requests outside the scope of support.

**Supported Program**: Refers to (a) any Software Release for which the associated initial Feature Release thereof (e.g., 3.0R 1.0) is less than 12 months prior to such Software Release and (b) the then most current shipping Software Release and 2 immediately prior versions of Maintenance Updates.

**TB:** terabytes delivered. One (1) TB is equal to 1,000 GB.

**Thps:** thousand Hits per second.

**Transaction Document:** Also known as PCR or SOW**,** refers to process for communicating and documenting a change to the scope of the Services purchased.

**User**: Any individual, application, API, or device that has interacted with the Edge Identity Cloud application, and Users are categorized into 3 types: Anonymous Users, Registered Users, and Monthly Active User.

EDGE DELIVERY SERVICES (OTHER THAN PROFESSIONAL SERVICES & SUPPORT)

**Account Protector**: Account Protector is designed to provide an integrated bot management and account takeover solution using a number of different techniques to (i) assess the risk of whether a human user is the legitimate account owner during the user authentication process and (ii) prevent fraudsters from accessing the account by allowing customer to apply different response actions based on user risk. Account Protector requires the purchase of one or more of the following services: Alta, KSD, DSA, DSD, ION, RMA, or WAA Services. As long as Customer maintains an active subscription for DDoS Fee Protection Service, the DDoS Fee Protection module shall also apply to Customer's Account Protector overage fees, if any, associated with DDoS attack.

**Adaptive Image Compression**: Adaptive Image Compression detects the current network conditions between a client and an edge server. It may dynamically re-compress image files, reducing file size and assisting in faster transmission of the image file.

**Adaptive Media Delivery**: Adaptive Media Delivery is optimized for adaptive bit rate streaming. This provides a high-quality viewing experience across varying network types and speeds, including mobile. Adaptive Media Delivery delivers both live and on-demand streaming media; and, since it's built on Edge Platform, it provides scalability, reliability, availability, and reach.

**Adaptive Media Player for Devices – Android SDK**: Adaptive Media Player for Devices (Android SDK) is a software SDK. It enables audio and video playback in popular Android-based mobile and TV platform formats. The software is delivered in executable format without source code, and configuration is performed by developers with available configuration objects, parameters, and client-side APIs.

**Adaptive Media Player for Devices – Premier**: Adaptive Media Player for Devices (Premiere) is a software SDK. It enables audio and video playback in popular mobile and TV platform formats. Premier includes business-critical third-party capabilities for monetization and measurement. The software is delivered in executable format without source code, and configuration is performed by developers with available configuration objects, parameters, and client-side APIs.

**Adaptive Media Player for Devices – Standard**: Adaptive Media Player for Devices (Standard) is a software SDK. It enables audio and video playback in popular mobile and TV platform formats. The software is delivered in executable format without source code, and configuration is performed by developers with available configuration objects, parameters, and client-side APIs.

**Adaptive Media Player for Web – Premier**: Adaptive Media Player for Web (Premiere) is a software SDK. It enables audio and video playback in popular web browser formats. Premier includes business- critical third-party capabilities for monetization and measurement. The software is delivered in executable format without source code, and configuration is performed by developers with available configuration objects, parameters, and client-side APIs.

**Adaptive Media Player for Web – Standard**: Adaptive Media Player for Web (Standard) is a software SDK. It enables audio and video playback in popular web browser formats. The software is delivered in executable format without source code, and configuration is performed by developers with available configuration objects, parameters, and client-side APIs.

**Advanced Cache Control (Advanced Cache Optimization)**: Advanced Cache Control optimizes the cacheability of complex content on the Edge Platform.

**Akamai Cloud (formally known as Linode): Compute Management Services**

- **Akamai Cloud API:** The Akamai Cloud API provides the ability to programmatically manage qualifying Akamai cloud products and services. This reference is designed to assist application developers and system administrators. Each endpoint includes descriptions, request syntax, and examples using standard HTTP requests. Response data is returned in JSON format by default.

- **Cloud Manager:** Cloud Manager is the user interface for deploying and managing virtual machines, configure networking, control user accounts, and access and configure qualifying Akamai Cloud Computing services. Cloud Manager supports you with: self-serve migrations so you can conveniently move your infrastructure between data centers; account management; updating payment information; reviewing credits remaining; printing invoices; sharing access to your cloud assets with your team by adding multiple users and configuring controls for each individual user; and managing your API Keys and add personal access tokens for more control over your Cloud Computing services. Please note: Cloud Manager does **not** manage non-Akamai Cloud services. A complete list of Akamai Cloud (Compute and Non-Compute) services are outlined in this document.

**Akamai Cloud (formally known as Linode): Compute Services (for purposes of the Compute SLA found here).**

- **Shared CPU:** Shared CPU instances are virtualized CPU cores that offer account-level allocated IPv4 and IPv6 addresses and standard Linux distributions. These resources are shared with other compute instances and a small amount of resource contention is possible.

- **Dedicated CPU:** Dedicated CPU cores offer optimized infrastructure for CPU-intensive applications. These Compute Instances are CPU-optimized and can sustain high CPU resource usage for as long as your workloads need. Dedicated CPU plans are ideal for production applications and CPU-intensive workloads, including high traffic websites, video encoding, machine learning, and data processing.

- **High Memory CPU:** High Memory CPU instances are Dedicated CPU cores optimized for workloads that value memory over CPU resources. High Memory Compute Instances are suitable for workloads that value much larger amounts of memory than other plans of a similar price. This includes any production application that requires large amounts of memory, in-memory database caching systems, in-memory databases, big data processing, and data analysis.

- **GPU:** GPU instances are dedicated virtual machines that offer GPU-optimized infrastructure for parallel processing workloads. The GPU-optimized virtual machines are accelerated by drivers such as the NVIDIA Quadro RTX 6000 to execute complex processing, deep learning, and ray tracing workloads.

- **Linode Kubernetes Engine:** The Linode Kubernetes Engine (LKE) is a managed container orchestration engine built on top of Kubernetes. LKE enables you to quickly deploy and manage your containerized applications without needing to build (and maintain) your own Kubernetes cluster. LKE instances are equipped with a fully-managed control plane at no additional cost. LKE instances feature automatic monitoring, backup, and recovery; a Kubernetes dashboard; and third-party integration.

- **TrafficPeak:** A packaged solution with Hydrolix services built on top of Akamai Cloud (previously Linode) and integrated with DataStream 2, SIEM, and other Akamai log and data services. TrafficPeak is an observability platform that can help customers visualize data in real-time to uncover deeper insights and enable their business transformation at a fraction of the cost.

- **Akamai Cloud (formally known as Linode): Non-Compute Services (for purposes of the Compute SLA found here). Backups:** A data backup service that is fully managed and stored server-side. Backups may be added to any customer instance provided that the host associated with the customer instance is not deleted. Up to four backups are stored as part of this service, including automated daily, weekly, and biweekly backups in addition to a manual backup snapshot. Each backup is a full file-based snapshot of your disks taken during your preferred scheduled time slot while the Compute Instance is still running. This means that the Backups service is not disruptive and provides you with several complete recovery options.

- **Block Storage:** The Block Storage service provides a method of adding additional storage drives to Compute Instances, enabling you to store more data without resizing your Compute Instance to a larger plan. These storage drives, called Volumes, can be formatted with any Linux-compatible file

system and attached and mounted to a Compute Instance. A Block Storage Volume augments the raw storage capacity of a cloud instance. Because a Volume is scalable, it can adapt as your data grows in size.

- **Cloud Firewall:** Cloud Firewall is a robust cloud-based firewall solution available at no additional charge for customers. Through this service, you can create, configure, and add stateful network-based firewalls to any Compute Instance. A Cloud Firewall sits between a Compute Instance and the Internet and can be configured to filter out unwanted network traffic before it even reaches your server. Defend your apps and services from malicious attackers by creating rules to only allow traffic from trusted sources. Firewall rules can filter traffic at the network layer, providing fine-grained control over who can access your servers.

  Control inbound and outbound traffic using the Cloud Compute API, Cloud Compute CLI or Cloud Manager. Each interface can be integrated into your workflow for seamless control over firewall rules. Cloud Firewall make security more accessible and enables you to secure your network traffic without needing to learn complicated software or even access the command line.

- **DDoS Protection:** DDoS Protection is a service included with Compute services which automatically detects DDoS (Distributed Denial-of-Service) attacks against Customer hosts. Always-on DDoS protection monitors, detects, analyzes, and blocks threats to the network in real-time. Attacks are blocked inline, then redistributed across Akamai's global fiber backbone. Rules are automatically created using machine learning from traffic across the global network to intelligently reroute malicious traffic during a DDoS event. Your server's applications are protected from a range of DDOS attack methodologies including UDP, SYN, HTTP floods, and more.

- **DNS Manager:** The Domains section of the Cloud Manager is a comprehensive DNS management interface, referred to as the DNS Manager. Within the DNS Manager, you can add your registered domain names and manage DNS records for each of them. In addition to supporting a wide range of DNS record types, the DNS Manager offers even more flexibility through AXFR transfers and zone types (primary and secondary). These two features work together so you can create a DNS configuration that works for your own application. Using Akamai as the primary DNS Manager is the most common option and allows you to manage DNS records directly on the Compute platform. Operating as a secondary DNS provider, you can manage your DNS records within other services or tools (like cPanel) but still host them on a Compute Instance, taking advantage of the reliability and high availability of our platform.

- **Harper DB**: HarperDB is a globally-distributed edge application platform. It reduces complexity, increases performance, and lowers costs by combining user-defined applications, a high-performance database, and an enterprise-grade message queue into a single package. HarperDB simplifies the process of delivering applications and the data that drives them to the edge, which dramatically improves both the user experience and total cost of ownership for large-scale application

- **Images:** The Images service allows users to store custom disk images in the Cloud. These images can be preconfigured with the exact software and settings required for your applications and workloads. Once created, they can be quickly deployed to new or existing Cloud Compute Instances.

- **Longview:** Longview tracks metrics for CPU, memory, and network bandwidth, both aggregate and per-process, and it provides real-time graphs that can help expose performance problems. The analytics and monitoring tool that is available in a free or pro (paid) format. Users can view a snapshot of 12 hours of historical data about their resources on up to 10 clients. Pro users can customize their views based on additional time frames and clients as priced. The Longview client is open source and provides an agent that can be installed on any Linux distribution–including systems not hosted by Akamai.

- **Macrometa**: Macrometa includes a suite of edge services powered by the Macrometa Global Data Network. The Macrometa Global Data Network (GDN) is a core feature of the Macrometa platform that enables the processing and analysis of real-time data from anywhere in the world. Macrometa services use the latest AI and Machine Learning developments to deliver a faster, more efficient, and secure online experience for users at enterprise scale without enterprise complexity.

- **Managed Databases:** Managed Databases allow you to quickly deploy a new database and defer management tasks like configurations, managing high availability, disaster recovery, backups, and data replication.

- **NodeBalancers:** NodeBalancers are managed load balancers as a service (LBaaS), making load balancing accessible and easy to configure on the platform. They intelligently distribute incoming requests to multiple backend Compute Instances, so that there's no single point of failure. This enables high availability, horizontal scaling, and A/B testing on any application on your Compute instance.

- **NVMe Block Storage:** NVMe Block Storage volumes are high-speed network volumes that offer scalable storage capacity manageable without a connected Compute instance and are available in the data centers indicated in the Cloud Manager.

- **Object Storage:** Object Storage is a globally-available, S3-compatible method for storing and accessing data. Under Object Storage, files (also called objects) are stored in flat data structures (referred to as buckets) alongside their own rich metadata. It does not require the use of a Compute Instance. Instead, Object Storage gives each object a unique URL with which you can access the data. An object can be publicly accessible, or you can set it to be private and only visible to you. This makes Object Storage great for sharing and storing unstructured data like images, documents, archives, streaming media assets, and file backups, and the amount of data you store can range from small collections of files up to massive libraries of information.

- **VLAN:** VLANs are private virtual local area networks that are available at no additional cost in select data centers. They operate on layer 2 of the OSI networking model and are entirely isolated from other networks. VLANs are a key part of enabling private and secure communication between Compute Instances on the Akamai cloud platform. They function like a virtual network switch, which means Compute Instances connected to the same VLAN can communicate with each other like they were directly connected to the same physical Ethernet network. Devices outside the network cannot see any traffic within the private network. Use the Cloud Manager to create a VLAN and assign Compute Instances. Create up to 10 VLANs per data center and assign each Compute Instance to up to 3 VLANs.

**API Acceleration**: API Acceleration is designed to provide API owners with a secure, resilient, and reliably scalable solution for their end-users.

**API Gateway**: The API Gateway helps Customer easily manage, govern, and scale APIs that are crucial for enabling new customer-focused business models. API Gateway leverages the Edge Platform to provide distributed access, policy, and traffic controls for API traffic. Since this work occurs on Edge Platform, it requires fewer round trips to origin, resulting in improved reliability and scale for APIs.

**API Security** (including Noname Security and Neosec): API Security solution is designed to protect all APIs regardless of where they run (on- or off-Edge Platform), alert teams to API vulnerabilities, and provide a unified inventory of all your APIs, with risk scoring. The solution also analyzes runtime API interactions for abnormal, suspicious, and malicious behavior, and enables real-time threat response remediation, and access to the last 30 days of API activity data. An additional managed threat hunting service called ShadowHunt enables leveraging the expertise of API Security professionals. API Security will analyze the amount of requests purchased (the "Usage Commitment"). The Usage Commitment is measured on a monthly basis. In the event Customer's usage of the API Security service exceeds the Usage Commitment in a given month, API Security will continue to analyze the requests until the number of requests exceeds the Usage Commitment by 200%. At that point, API Security will no longer analyze any further requests over this limit during such month. API

Security is not designed to capture all requests during periods of large upward volatile and irregular changes in request traffic and therefore may not ingest all requests during such an event. Non-captured requests will not count against a Customer's monthly Usage Commitment.

**App & API Protector (AAP)**: App & API Protector is designed to improve the security posture of Customer protected web domains by reducing the likelihood and impact of application-level and denial-of-service attacks by intercepting suspected malicious traffic in the Edge Platform before it reaches the Customer's protected domains. AAP includes rate control protections to help mitigate the risk of DoS and DDoS attacks as well as common attack methodologies such as SQL injection, cross-site scripting, Trojan backdoors, and malicious bots. AAP also includes the following features:

- "Slow POST" protection
- Network layer controls
- Application layer controls
- Bot visibility & mitigation controls
- Adaptive Security Engine with automatic update, self-tuning, and tuning recommendations
- Security Center includes traffic dashboards and data analytic features
- Security Foundation (ASF) which consists of API Discovery, Beta Channel, and SIEM Integration.

Kyndryl may require sampling for custom visibility/monitoring rules, in which case Kyndryl will notify Customer and assist with the configuration change.

**Advanced Delivery**: Advanced Delivery is an optional add-on to AAP that Includes Ion as a delivery product.

**Advanced Security Management (ASM)**: Advanced Security Management is an optional add-on to AAP that is designed to complement AAP by providing additional security configurations, security policies, and rate controls. ASM supports a number of advanced features that make it possible to address demanding security requirements including API registration (for positive API security), path-based policy matching, Client Reputation signals, and manual policy evaluation for the Adaptive Security Engine.

**Malware Protection:** Malware Protection is an optional add-on to AAP, AAP with ASM, Kona Site Defender, and Web Application Protector that is designed to mitigate the impact of malicious file uploads sent via HTTP(S) by detecting and intercepting suspected malicious uploads in the Akamai network beforethey reach the Customer's protected domains. Customers then have the option to apply an action to the files suspected as malicious.

**Audience Hijacking Protector**: Audience Hijacking Protector is designed to prevent unwanted redirection to malicious websites, while simultaneously giving customers the ability to allow or deny any browser extension.

**Beta Channel**: Customer hereby agrees to participate in a program which provides ongoing access during the term of this Order Form (the "Beta Channel Agreement") to a limited set of Edge Delivery Services products, services and software designed for pre-release beta ("Beta Offerings") as they become available (the "Beta Channel"). Beta Offerings provided via the Beta Channel shall constitute Services for purposes of the terms in the Agreement; however, the provisions of this Beta Channel Agreement below supersede any conflicting provisions in the Agreement. Customer will enable and disable their specific Beta Offerings via the EdgeControl Management Center portal, at Customer's sole discretion. For purposes of clarity, this Beta Channel Agreement shall govern all Beta Offerings that Customer enables. Beta Offerings are provided "as-is" without express or implied representations or warranties of any kind including, without limitation, any warranties set forth in the terms and conditions.

Kyndryl shall provide reasonable support for Beta Offerings; however, Customer acknowledges that Beta Offerings are still in development and may contain errors and limitations and that no warranty or service level agreement shall apply. Customer further acknowledges that Beta Offerings are independent and distinct from Kyndryl's generally available products, services and software. Kyndryl reserves the right to change and/or remove Beta Offerings from the Beta Channel at any time with notification by electronic mail to Customer if

they have enabled such Beta Offering. Should Kyndryl offer a production version of a Beta Offering (the "Commercial Offering"), it shall replace the Beta Offering with the Commercial Offering, and Customer will have the option to purchase the Commercial Offering unless it is automatically packaged into its Edge Delivery Services at no charge in Kyndryl's sole discretion. Customer will have no less than sixty (60) calendar days to execute the option to purchase the Commercial Offering and Kyndryl will provide access to and support of the Commercial Offering to Customer during such sixty (60) day period.

**Bot Manager (i.e., Bot Manager Standard, Bot Manager Premier, and Bot Manager Premier Mobile Protection Module)**: Bot Manager is designed to use a number of different detection techniques in order to: (i) determine if a client making a port 80 HTTP or port 443 HTTPS request on the Edge Platform is a human or a bot and (ii) categorize the bots into known bot categories and unknown detected bot categories. Customer may set policies to apply different response actions to different categories of bot traffic. Bot Manager requires the purchase of one or more of the following Services: KSD, DSA, or Ion. As long as Customer maintains an active subscription for DDoS Fee Protection Service, the DDoS Fee Protection module shall also apply to Customer's Bot Manager overage fees, if any, associated with DDoS Attacks.

**China CDN**: China CDN is a performance solution that allows delivery of content within China from Edge Platform servers located in China and additional servers outside China. Without the China CDN Service, all content is delivered from Edge Platform servers outside China. Kyndryl reserves the right to limit or restrict the amount of traffic purchased for delivery via Russia CDN and/or China CDN Services. Customers using Russia CDN and/or China CDN Services shall comply with all applicable laws in Russia and/or China, including without limitation: (i) laws that address the storage of any personal information inside Russia and/or China; and (ii) registration requirements for .ru and/or .cn sites. Customer agrees to supply Kyndryl with all documentation or registration-related information (including origin IP addresses) reasonably requested by Kyndryl. Kyndryl provides no guarantee or warranty that the Russia CDN Service or China CDN Service shall be delivered from within Russia or China, respectively. Kyndryl may deliver all or part of the China CDN Service with the use of third party suppliers, which may collect their own log files.

**Client Access Control Module (CAC)**: CAC supplies a set of IP addresses that Edge Platform uses to serve Customer content. As these IP addresses change over time, CAC includes an interface where the Customer can manage these changes.

**Client Reputation**: Client Reputation is designed to help protect online applications from attacks, improve accuracy, and fight threats. Client Reputation computes risk scores associated with Customer's end user clients and allows Customer to filter malicious end users based on risk scores. Client scores are updated periodically but are neither real-time nor per event. Client Reputation requires Kona Site Defender.

**Client-Side Protection and Compliance**: Client-Side Protection & Compliance is a detection-first solution that is designed to detect changed, malicious, and compromised JavaScript resources that could be used to steal user data or deface the user experience, and helps customers reach compliance with PCI DSS v4 requirements 6.4.3 and 11.6.1. Client-Side Protection & Compliance notifies security teams with actionable insights, empowering them to rapidly understand and act on the threats.

**Cloud Embed**: This Service can help cloud provider seamlessly integrate core features of Edge Platform's content delivery platform into its cloud environment via application program interfaces and offer its customers delivery capabilities powered by Edge Platform's global network of servers. In optimizing the delivery of cloud-hosted workloads, Cloud Embed is designed to support the delivery of whole websites or applications and included objects, automatically scale delivery globally to handle high traffic loads during peak usage periods, and remain available 24/7 regardless of Internet conditions.

**Cloudlet**: A Cloudlet is a specialized and discreet functionality designed to enhance Customer's delivery service. To purchase any Cloudlet, Customer must have purchased one or more of the following Services: DSA or Ion.

**Cloudlet – API Prioritization**: API Prioritization reduces abandonment by maintaining continuity in user experience during unexpected peak demand. It does this for applications that call non- HTML assets through back-end API or other service calls.

**Cloudlet – Application Load Balancer**: Application Load Balancer can automatically detect load conditions, then route traffic to the optimal data source. It helps provide consistent visitor session behavior without load feedback from origin.

**Cloudlet – Audience Segmentation**: Audience Segmentation provides hassle-free traffic segmentation and session stickiness without degrading performance. Customer can use Audience Segmentation for A/B and multivariate testing and to provide a personalized customer experience. Customer can manage various audience segments and quickly make changes.

**Cloudlet – Cloud Marketing**: Cloud Marketing helps transfer data collected by Customer's MediaMath configuration code. Edge Platform injects this code into Customer's HTML documents and shares any resulting data with MediaMath, Inc.

**Cloudlet – Cloud Marketing Plus**: Cloud Marketing Plus helps transfer data collected by Customer's MediaMath configuration code. Edge Platform injects this code into Customer's HTML documents and shares any resulting data with both MediaMath, Inc. and its third-party partners.

**Cloudlet – Edge Redirector**: Edge Redirector assists IT staff and marketing web site owners who manage a high number of URL redirects. Edge Redirector is a redirection tool that provides a simple user interface to quickly and easily manage URL redirect logic using a flexible set of rules and match criteria, while decreasing time to redirect from the edge platform, effectively reducing round trips and providing additional origin offload. Unlike DIY or third party solutions, Edge Redirector takes advantage of the platform providing additional scale and performance in addition to offload.

**Cloudlet – Forward Rewrite**: Forward Rewrite helps website owners boost search engine optimization by creating human-readable and search engine friendly URLs for dynamically generated pages. Edge Platform rewrites the requested URL on the Edge Platform in order to return a different asset or origin based on a number of conditional rules while keeping the URL shown to the visitor in the address bar unchanged.

**Cloudlet – Input Validation**: Input Validation evaluates web form submissions against customizable recipes and limits excessive valid or invalid attempts. It is designed to protect against behavioral or brute force attacks helping Customer to avoid business disruption, reduce custom development, and gain additional application offload.

**Cloudlet – Phased Release**: Phased Release can help facilitate a fast rollout of code changes to production with real users. It lets Customer gradually move visitors to a new experience or deployment and provides the ability to fail back immediately if there are problems. If Customer has frequent software releases or uses canary deployments, Phased Release can help reduce risk and speed time to market.

**Cloudlet – Request Control**: Request Control uses allow lists and deny lists to help offload unqualified traffic from the origin. The allow lists and deny lists use the inbound HTTP request criteria selected by Customer. Managing the evaluation of these requests via the Edge Platform provides additional security, offload, and operational agility.

**Cloudlet – Visitor Prioritization**: Visitor Prioritization provides a branded waiting room experience for high-demand applications. It provides granular control of incoming traffic to help prevent application overload. If applications experience traffic surges, Visitor Prioritization lets Customer use its existing resources to create a positive user experience.

**CloudTest**: CloudTest is a combination of Edge Delivery Service and software installed on hardware and, as applicable, software that is required to run the CloudTest software. CloudTest is designed for (i) internally

testing Customer's websites and web-based and mobile applications behind Customer's firewall, and (ii) externally testing Customer's websites and web-based and/or mobile applications.

**CloudTest On Demand**: CloudTest On Demand is a managed service designed for testing Customer's websites, web-based applications, and mobile applications. With CloudTest On Demand, CloudTest software runs on the Edge Platform, letting Customer run both internal and external tests from behind its firewall.

**CloudTest Server Hours:** Customer can purchase compute hours from Kyndryl at an hourly rate for the sole purpose of running tests from the CloudTest On Demand Service. Requires purchase of CloudTest On Demand.

**Cloud Wrapper**: Cloud Wrapper is designed to help Customer more effectively manage Edge Delivery Service's interface to its origin services. It works with both private origins and public cloud origins. Cloud Wrapper is an integrated part of the tiered caching infrastructure. Customer purchases a cache capacity reservation and selects the geography during onboarding. The reservation is maintained in a distributed fashion within that geography. Cloud Wrapper uses Customer's allocated space expressly for caching Customer's content using otherwise standard caching practices to help improve origin offload and prevent traffic spikes. Assets not accessed within a 30-day period may be subject to cache eviction.

**Compliance Management**: Compliance Management helps Customer understand how Edge Delivery Services relate to Customer's compliance initiatives. It provides documentation that maps EDS policies and procedures to sections of specific compliance frameworks. Documentation may be requested through Customer's account team. Available framework modules are:

- **PCI**: This module provides the following documents:
  - A copy of the Attestation of Compliance issued upon completion of its most recent PCI audit; and
  - An executive summary of recent quarterly network vulnerability scans performed on the Edge Platform SSL network.
- **ISO**: ISO 27002 is a set of guidelines for information security management. This module includes an executive summary from the most recent ISO 27002 assessment and selected documentation about the EDS policies and procedures reviewed. An assessment against ISO 27002 does not measure the effectiveness of any policies. Instead, it verifies that policies are well documented,
    - clearly communicated, and universally followed.
- **FISMA**: This module includes documentation on EDS policies and procedures reviewed as part of the Federal Information Security Management Act (FISMA) self- assessment effort against NIST 800-53.
- **BITS**: This module includes documentation on EDS policies and procedures reviewed for the BITS self-assessment. BITS is part of the Bank Policy Institute.
- **HIPAA**: This module includes documentation on EDS policies and procedures relevant to the Health Insurance Portability and Accountability Act (HIPAA).

**Compliance Management – On Site Audit**: On-Site Audit Compliance Management is delivered by team at offices in Cambridge, Massachusetts over a period of up to 5 consecutive business days, and it provides a deeper review of EDS' policies and procedures relative to the Customer.

**Content Protector**: Content Protector is designed to use a number of different detection techniques in order to determine if a client making a port 80 HTTP or port 443 HTTPS request at the Edge is a human or a bot. Customer may set policies to apply different response actions to different of bot traffic classification segments. Additional Content Protector Terms: Content Protector requires the purchase of one or more of the following services: AAP, AAP+ASM, any delivery product and BMS, any delivery product and BMP, any delivery product and APR, any delivery product and KSD. As long as Customer maintains an active subscription for DDoS Fee Protection Service, the DDoS Fee Protection module shall also apply to Customer's Content Protector overage fees, if any, associated with DDoS attacks.

**Content Targeting**: Content Targeting enables Customer to customize content to individual end users. It accurately identifies the end user's geographic location, network type, and network condition so that content can be targeted in real time on the Edge Platform for each visitor. It also is designed so that the content should only be served to authorized users.

**DataStream**: DataStream offers real-time visibility into CDN performance, and it is designed to empower organizations to increase release velocity with the insights and agility to detect and resolve issues that arise in real-time. DataStream provides raw logs through PUSH API for agile and reliable DevOps practices for a Customer's CDN configurations and digital applications.

**DDoS Fee Protection**: DDoS Fee Protection provides Customer with a credit for overage fees incurred due to a DDoS Attack. For eligible requests, Customer's overage fees for the month in which the DDoS Attack occurred are reversed and replaced with the Capped Burst Fee set forth on the applicable Transaction Document (unless actual overage fees are less than the Capped Burst Fee amount, in which case the actual overage fees will apply). DDoS Fee Protection is available as part of Kona Site Defender, Kona DDoS Defender, and Web Application Protector. DDoS Fee Protection is not available to Customers that receive consolidated invoices aggregating usage from more than one Service or Transaction Document. To be eligible for a credit: (a) the DDoS Attack must result in overage charges in excess of twice the average monthly overage fee measured in the preceding six months, excluding months in which a mutually agreed DDoS Attack occurred, (b) Customer must notify Kyndryl's technical support organization of the DDoS Attack, (c) Kyndryl's technical support organization must verify that any such reported DDoS Attack is eligible for credit, and (d) the credit requests must be submitted no later than 30 days following a disputed Service invoice. When issuing a credit, Kyndryl shall have sole authority in determining whether the reported Service incident qualifies for credit. If Customer's average monthly Service fee exceeds its selected tier, or if more than two credits are requested in any given calendar year, then Kyndryl shall have the right to require Customer to pay a higher Capped Burst Fee. A single credit shall be applied on a monthly basis, even when multiple DDoS Attacks occur in the month. Credit shall be issued as a credit memo and not a revised invoice.

**Device Characterization**: Device Characterization provides Customers with characteristics drawn from an EDS database of mobile devices matched via the Edge Platform.

**Download Delivery**: Download Delivery is a reliable, high performance content delivery solution for large-sized files (>100MB). It is designed to deliver superior capacity, scalability, availability, and performance. Download Delivery includes metrics and optional tools for monitoring and managing the download process across a customer base, offering a predictable, high-quality download experience while helping to address online distribution goals.

**Dynamic Page Caching**: Dynamic Page Caching allows Customer to condition cache pages based on URI, query strings, cookies, and request headers.

**Dynamic Site Accelerator (DSA)**: DSA helps improve the reliability, offload, and network performance of Customer's original web infrastructure while handling the specific requirements of dynamically generated content. DSA speeds and secures interactive web sites, helping Customer scale to meet sudden needs, like holiday shopping or flash sales, without adding hardware.

**Edge Connector for Salesforce® Commerce Cloud**: The Edge Connector for Salesforce Commerce Cloud helps Customer maintain its existing Edge Delivery Service while communicating directly with Salesforce Commerce Cloud. Edge Delivery Service is the only approved alternative to the embedded content delivery network for Salesforce Commerce Cloud. Used together, Edge Connector and Salesforce Commerce Cloud can help Customer increase customer engagement with personalized online experiences, gain IT agility, scale globally, and increase revenue opportunities.

**Edge Device Characterization**: Device Characterization provides information about the type of device used to send a request. To support Device Characterization, EDS maintains a database of mobile devices.

**Edge DNS**: Edge DNS is a cloud-based authoritative DNS solution designed to augment or replace a Customer's existing DNS infrastructure. Edge DNS helps improve DNS resolution times, especially for websites using an Edge Delivery Services. It also has the scale to absorb large DDoS attacks targeting the DNS infrastructure.

**Edge DNS Security Option**: The security option of Edge DNS provides the following additional services:

**Edge DNS Sign and Serve DNSSEC**: Enables transfer of unsigned zone from Customer's hidden master DNS server to EDS. Requires annual update of a signing key reference called a DS record.

**Edge DNS Serve DNSSEC**: Enables transfer of signed zone to EDS for serving DNSSEC queries.

Edge DNS limits the number of zones to 2,000. Exceeding 2,000 zones is configurable by a request. Edge DNS zones may have up to 25,000 records per zone. Additional records per zone is configurable by a request. Unless otherwise specified in the applicable Transaction Document, a Customer is entitled to 2 billion hits per month across all their zones. Unless otherwise specified in the applicable Transaction Document, DNS zones hosted on Edge DNS may only be used for zones owned by the Customer. Delivery of the Service is evidenced by the provisioning of the Customer's customer portal access credentials.

**Edge Identity Cloud (AIC)**: AIC provides a highly secure and resilient environment for processing user sign-ins and collecting and storing sensitive identity information at large scale. For this solution, usage associated with Customer applications are subject to overage charges exceeding their usage allowance, as specified in the applicable Transaction Document.

Additional Terms:

- AIC support in the China region with the limitation of no encryption at rest for a Customer's personally identifiable information stored in the region.
- AIC offers support for the Russian region in compliance with the Federal Law No. 242-FZ and No. 152-FZ on Amendments to Certain Legislative Acts of the Russian Federation Clarification of Personal Data Processing in Information and Telecommunication Networks. The Identity Cloud Russia solution provides a "write first in Russia" approach, with the application hosting and data storage of Customer's personally identifiable information taking place in a secondary region in the EU. The EU region must be added when deploying the Russian region.
- Customer shall not use AIC to store personal health information, financial account numbers, credit account numbers, or government-issued personal identification numbers (like social security and driver's license numbers).
- Use of AIC is based on a shared tenancy model. Customers requiring single-tenant deployments may purchase a supplemental option for single tenancy.
- AIC includes up to 3 environments (also known as "registration apps") per region to support development, staging, and production activities.
- AIC includes one Customer Insights production environment per region and 5 Customer Insights seats in total. Customers requiring greater numbers may subscribe for additional seats. Kyndryl will periodically review Customer Insight seat usage and deprovision inactive accounts.
- Each AIC Customer is subject to a maximum average daily transaction quota so as to protect the service for all users, where a transaction is a single call or request to an AIC endpoint or supporting system in which a request is made and a response is returned, successful or not. ● The quota is designed to protect against denial-of-service attacks and help ensure that adequate resources are available for all customers. AIC includes entitlement for a maximum average daily transaction quota of 10 transactions per second, during a calendar month. Rate quotas are subject to change to protect customers, at Kyndryl's discretion. Kyndryl will provide advance notice of such changes when possible. Customers requiring higher rate quotas may subscribe to the Dynamic Performance Option.
- AIC can support custom JavaScript Injection. This requires pre-approval from the Kyndryl account team, and the customer assumes all risk related to the use of custom JavaScript in AIC.

**Edge IP Binding**: Edge IP Binding allows Customer to configure hostnames to a limited set of IP addresses provided by EDS.

**EdgeKV**: EdgeKV is a distributed key-value store that enables JavaScript developers to build data-driven EdgeWorkers applications for latency-sensitive use cases. Customers are responsible for maintaining control over the data hosted on this Service and for appropriately using the data returned by EdgeKV. EdgeKV does not support storage of sensitive information where the consequence of an unauthorized disclosure would be a serious business or compliance issue. Customer should not use sensitive information when creating namespaces, groups, keys, or values.

**Edge MFA**: Edge MFA is designed to use various authentication factors to provide user authentication services. Customers may set policies to apply different authentication requirements to different groups of users.

**EdgeScape (i.e., EdgeScape, EdgeScape Pro, EdgeScape Enterprise, and EdgeScape Enterprise Pro)**: EdgeScape provides access to the EdgeScape Database, which includes EDS proprietary information that can be used to assess the geographic and network points-of-origin of Site requests. The EdgeScape Database shall provide the following information: country code, region code (US state/non- AOL only and province (Canada only)) and network and connection type for certain networks (as selected by Kyndryl). Customer shall not integrate both the Identification Codes and IP addresses obtained from the EdgeScape Database with any of its databases or provide both the Identification Codes and the IP addresses to a third party.

**EdgeWorkers**: EdgeWorkers enables a Customer's developers to not only create their own services using JavaScript, but also to deploy them across the Edge Platform. Deploying code at the edge brings data, insights, and decision-making closer to the users and systems that act upon them. By enabling EdgeWorkers, development teams expand their ability to build services and manage Edge Platform as part of their digital infrastructure.

**Enhanced Protocol**: The Enhanced Protocol is a suite of advanced routing and transport optimizations that are designed to increase Customer's website's performance and reliability.

**Enhanced TLS**: Enhanced TLS delivers an HTTP (HTTP over TLS) service on an SSL network and is designed to encrypt data in transit and validate the identity of the delivery server using Customer's TLS certificates. It includes one of the following Digital SSL Certificates: DV-SAN, DV-SAN-SNI, OV, OV-SNI, OV-SAN, OV-SAN- SNI, EV, EV-SNI, EV-SAN, EV-SAN-SNI, Wildcard, Wildcard-SNI, Wildcard-SAN, Wildcard-SAN-SNI.

**Enterprise Application Access (EAA)**: EAA provides end user access to private intranet applications from outside the protected corporate network. It integrates data path protection, identity access, application security, and management visibility and control into a single service. EAA authenticates users to allow secure access to private applications deployed either to Customer's datacenter or on Customer's public IaaS. It enables access only to provisioned web, RDP and SSH applications. It does not grant full network access. This application lets Customer close all inbound firewall ports, which hides applications from the Internet and public exposure.

**Enterprise Defender**: Enterprise Defender helps organizations deploy Zero Trust service architectures that eliminate perimeter security models and provide protections for users against Internet-based threats such as malware. It simultaneously protects and accelerates access for users as they communicate with corporate applications and data. Enterprise Defender includes EAA Enterprise, ETP Advanced Threat, Kona Site Defender, and IP Accelerator.

**Fast-IP Blocking (FIPB) Module for IPA/SXL**: The FIPB module is designed to provide control over the traffic that reaches Customer's origin servers by filtering traffic from pre-specified sources. It includes access to one or more of the following network layer controls:

- A list of IP addresses that are explicitly denied a connection to an edge server (i.e., an IP deny list)

- A list of IP addresses that are explicitly accepted without further security analysis (i.e., an IP allow list)
- Strict IP Whitelist, a configuration option within the Kona Web Application Firewall network-layer controls in which requests are processed solely for the IP addresses within the IP allow list, whereas requests from all other IP addresses are explicitly denied a connection to an edge server
- Controls, a configuration option within the Kona WAF network-layer controls in which requests from a source IP address can be explicitly denied based on the country from which the request originates

**Foreground Download**: Foreground Download helps to accelerate the delivery of downloaded media and large files, such as software and games. The Service is designed to improve throughput that would impact download times as experienced by end users.

**Global Traffic Management (GTM) Standard**: GTM applies an Internet-centric approach to global load balancing and helps Customer's users more reliably access Customer's websites and IP applications. Unlike traditional hardware-based solutions that reside within the data center, GTM is a fault-tolerant solution that makes intelligent routing decisions based on real-time data center performance health and global Internet conditions. Based on this data, the Service routes online user requests to the most appropriate data center using an optimized Internet route for that user at that moment. It uses the scale and speed of the Edge Platform to help provide high site availability and responsiveness.

> **GTM IPv6 for Global Traffic Management**: This module is included with GTM Standard. It lets GTM Properties test with and respond to IPv6 requests, like AAAA requests. This module includes an IP version selector rule type that responds to both A and AAAA requests.

**GTM Premier**: GTM is designed so that Internet users can more reliably reach Customer's websites and other IP applications. It applies an Internet-centric approach to global load balancing to provide high site availability and responsiveness to online user requests. Unlike traditional hardware-based solutions that reside within the data center, GTM is a fault-tolerant solution that makes intelligent routing decisions based on real-time data center performance health and global Internet conditions. Based on this data, the Service routes online user requests to the most appropriate data center using an optimized Internet route for that user at that moment. It's the only load balancing solution that leverages the scale and speed of Edge Platform**.**

> **GTM Premier Load Feedback**: Available with GTM Premier, this feature helps prevent datacenter overload. It uses current load feedback to dynamically change the amount of traffic sent to a target. It works as long as you have the capacity needed to fulfill the request. A GTM Datacenter exists within the context of a GTM Domain but may be used by all GTM Properties within that GTM Domain.

Unless otherwise specified on the applicable Transaction Document, Customer is entitled to 100 GTM Properties and 2 billion hits per month across all its GTM Domains. Additional GTM Properties are available by a request.

**Global Traffic Management Protect & Perform**: Combining the features and modules of GTM Standard and Premier, Global Traffic Management Protect & Perform is designed to ensure that Internet users can more reliably get to your websites or any other IP application. It applies an Internet-centric approach to global load balancing to provide high site availability and responsiveness to online user requests. Unlike traditional hardware-based solutions that reside within the data center, Global Traffic Management service is a fault-tolerant solution that makes intelligent routing decisions using real-time data center performance health and global Internet conditions to route requests to the most appropriate data center using an optimal Internet route for that user at that moment.

**Guardicore Security Platform** is a security solution that is designed to enable Customer to apply microsegmentation to minimize the effects of breaches, like ransomware, and provides network flow visibility and policy enforcement. The solution is offered on licensed or Software-as-a-Service ("SaaS") basis and is comprised of the following components and service:

- **Guardicore-Agents-Servers** - Software modules deployed on standard Windows and Linux servers.

- **Guardicore-Agents-EndPoint** - Software modules deployed on standard Windows and Linux endpoints.
- **Guardicore-Management** - Management system instance that manages the Agents and provides configuration and control for the platform. Provided on a per instance basis with available additional instances for on-premises, disaster recovery instance, and lab\staging management).
- **Guardicore-Integration** - Third party integrations can be purchased as part of the solution (e.g., F5, Citrix, AS400, Switch). Integrations are priced separately.
- **Guardicore-Add-Ons** - Additional capabilities in the product that are priced separately (e.g., Deception, Insight, application portal, additional storage).
- **Guardicore-Other** - Additional available services (e.g., professional services packages, Labs packages, Support tier packages).

**HTTPS – Shared Cert**: This Service provides HTTPS access for content delivered using Adaptive Media Delivery and Download Delivery. It uses hostname matching based on one of the wildcard entries on the shared certificate. It requires an EDS-owned SAN digital certificate.

**Image and Video Manager**: Image and Video Manager is designed to help Customers with the creation and management of their images and videos. The Image and Video Manager Service provides Customers with an interface to call graphical manipulations on images and videos according to a Customer-designed policy. Customer images and/or videos shall be supplied by Customer on origin web servers or uploaded to NetStorage and must be delivered utilizing Edge Delivery Services.

**Ingest Acceleration**: Ingest Acceleration is a feature of MSL3 and MSL4 that allows Customer to use EDS' proprietary transport protocol to push live media streams to the Edge Platform.

**Ingestion**: Ingestion is a feature of MSL3 and MSL4 that allows live content (in HLS, HDS or DASH) to be passed through the EDS network without manifest or format manipulation.

**Integrated Cloud Accelerator**: Integrated Cloud Accelerator is an option of Cloud Embed that includes access to EDS' network for content delivery and content acceleration for Cloud Partners. It provides features designed for origin offload and the delivery of content over HTTP and HTTPS.

**Ion Standard (Ion)**: Ion is a suite of intelligent performance optimizations and controls that helps deliver superior web, iOS, and Android application experiences. Built on the SLA-backed availability of EDS' globally distributed platform, Ion continuously monitors real user behavior, automatically applying best practice performance optimizations and adapting in real time to connectivity, content, and user behavior changes.

**IoT Edge Connect**: IoT Edge Connect provides a distributed, MQTT broker service. IoT Edge Connect is designed to be connected to an ISO compliant (ISO/IEC 20922:2016) MQTT 3.1.1 client. IoT Edge Connect also supports a capability to connect to the broker service via HTTPS 1.1. Messages received by the broker are made available as a data stream with a defined data retention storage allowing for devices and data centers to re-synchronize state after periods of disconnection.

**IP Application Accelerator (IPA)**: IPA helps enterprises deliver IP applications to globally distributed users quickly, securely, and reliably, without the expense of building out and supporting dedicated IT infrastructure. A managed service, IPA delivers high application availability and consistent online response times worldwide. It also supports hosting and SaaS providers that provide cloud-based IP applications such as remote desktop management, hosted email, and archiving. Built on the Edge Platform, IPA leverages technologies that improve delivery of TCP/IP applications by overcoming the public Internet's real-time latency, packet loss, and transport inefficiency.

**IPv6 Feature**: IPv6 Feature provides HTTP delivery, and HTTPS delivery for secure delivery products, of content and applications on a dual-stack hostname/digital property (such as *www.example.com)* for which DNS name servers respond to A and AAAA requests with corresponding edge servers capable of serving IPv4 and IPv6 HTTP(S) requests. IPV6 Feature, which includes access to customer portal, helps Customer set up dual-stack hostnames and provide applicable IPv6 visitor and traffic reporting.

**IPv6 Module for IPA/SXL**: This module provides IP application delivery (including HTTPS delivery for SXL) of content and Applications on a dual-stack hostname or dual-stack digital property such as *www.example.com*. EDS DNS name servers respond to both A and AAAA requests with corresponding edge servers capable of serving both IPv4 and IPv6 requests. It allows access to the customer portal to set up dual-stack hostnames and provide applicable IPv6 visitor and traffic reporting.

**Jump Point Navigation/Random Seek**: This option allows for random seek within progressively downloaded videos.

**Kona DDoS Defender**: Kona DDoS Defender is designed to protect individual web properties against common DDoS Attacks by absorbing and deflecting such attacks and authenticating valid traffic at the network edge. The Service supports protection of port 80 HTTP and port 443 HTTPS traffic. Kona DDoS Defender is managed by the SOCC and includes limited customer self-service capabilities.

Additional Kona DDoS Defender Terms:

- Protection Policies for Kona DDoS Defender include “Slow POST” protection, rate controls, and network layer controls.
- The Kona DDoS Defender solution includes the following companion features delivered by the SOCC: Kona DDoS Defender Configuration Assistance, Kona DDoS Defender Security Event Monitoring, Kona DDoS Defender Attack Support, Kona DDoS Defender Emergency Configuration Assistance, and Kona DDoS Defender Table Top Attack Drill
- Site Shield Maps created as part of the Kona DDoS Defender entitlement are not supported with the China CDN Service
- Any Customer requests for Kona DDoS Defender customizations to be made outside the context of an SOCC-confirmed DDoS Attack shall be considered out of scope.
- Kona DDoS Defender only provides protection for DDoS Attacks. Protection for application- level attacks through Kona Web Application Firewall rules, including but not limited to brute force login attempts or SQL injection attacks, is not included.

**Kona DDoS Defender Change Management Process**: As part of the Kona DDoS Defender Change Management Process, Kyndryl may, as needed to expedite the response to DDoS Attacks, make any of the Emergency Security Configuration Assistance changes or customizations to the Customer’s configuration in order to defend against confirmed DDoS Attacks. All other changes will require an associated approved change ticket within the ticketing system.

**Kona DDoS Defender Configuration Assistance**: Kona DDoS Defender is configured by Kyndryl during integration. Customer’s configuration will be completed using a standardized configuration template suitable for Customer’s protected properties and traffic type. Rate control thresholds will be configured based on Kyndryl’s defined Kona DDoS Defender High Alert threshold. The threshold may be evaluated and adjusted up to two additional times each contract year as part of standard maintenance that is not attack related.

**Kona DDoS Defender Emergency Configuration Assistance**: In connection with this Service, Kyndryl will, for any EDS SOCC-confirmed DDoS Attacks, implement configuration changes as needed to mitigate the DDoS Attack's adverse effects on the Customer’s protected web properties. The following changes may be made in response to confirmed DDoS Attacks: (i) rate control management and tuning, (ii) block and allow list management, (iii) geographic list management, and (iv) configuration of slow post mitigations. Once a confirmed attack has been mitigated and ongoing attack activity subsided, any of the above customizations may be reversed as mutually agreed between Customer and the SOCC at no additional cost to Customer.

**Kona DDoS Defender Security Event Monitoring and Attack Support**: This Service provides near real time analysis of log events originating from available Kona DDoS Defender alerts on a 24x365 basis. A Security Event is initiated by a high threshold alert triggering to the SOCC. Once a Security

Event has been recognized and categorized as security relevant, Kyndryl's monitoring system opens a Security Incident from the log event and opens a ticket within the EDS ticketing system. This ticket shall be analyzed by security response staff and escalated to Customer if it is not possible to classify the Security Incident as a false positive.

**Kona DDoS Defender Table Top Attack Drill**: The Table Top Attack Drill is an exercise between the SOCC and Customer whereby an attack scenario is reviewed in order to confirm communication workflow, escalation path, and operational agility. Up to 1 Table Top Attack Drill per year is included only if Customer experiences no confirmed attacks during the contract year.

**Kona Site Defender**: Kona Site Defender is designed to improve the security posture of Customer's protected Domains and API endpoints and reduce the likelihood and impact of application level and denial of service attacks by mitigating attacks in the EDS network before they reach Customer's origin infrastructure. Kona Site Defender includes configurable functionality designed to protect Customer Domains by reducing the risk and impact of attacks at the network and application layers. Kona Site Defender provides rate control protections to mitigate the risk of DoS and DDoS Attacks as well as common attack methodologies such as SQL injection, cross-site scripting, Trojan backdoors, and malicious bots. The specific security controls included in Kona Site Defender include, "Slow POST" protection, rate controls, network layer controls and application layer controls. Kona Site Defender provides tools that enable the definition and enforcement of security policies specific to client IP, HTTP method and other request parameters. Kona Site Defender is also designed to provide protection from burst charges associated with unexpected or malicious traffic spikes. Kona Site Defender includes Kona Web Application Firewall, Site Shield, Site Failover, Access Control, Security Monitor and DDoS Fee Protection.

**Kona Third Party Management Access**: This option allows Customer to assign a named third party to access and manage Customer's configuration on its behalf. Third Party Management Access option is available for the Web Application Protector and Kona Site Defender family of Services.

**Log Delivery Service**: Log Delivery allows Customer to retrieve logs generated from various Services. Customer can configure how to receive their deliveries in the customer portal.

**Manifest Personalization**: Manifest Personalization enables Customer to optimize playback experiences and tailor streaming content at a user, device, geo, or network level by dynamically manipulating the manifest via the Edge Platform. Customer can personalize manifests in a scalable way by offloading this function to the EDS network, reducing the associated computation and storage overhead on the origin service.

**Media Analytics**: A cloud-based, self-service, client-side solution that provides visibility into online video (live events, 24/7 live linear streams, or video on-demand) performance, quality of experience, and audience behavior by monitoring crucial metrics that power media business decisions. Media Analytics is comprised of two key modules (Quality of Service-QOS-Monitor and Audience Analytics) that help content providers assess their business by providing data and insights to retain, track, monetize, and further engage their online audiences.

**Media Analytics – Audience Analytics Module**: Audience Analytics provides a comprehensive overview of key audience behavior trends with 13 months of historical data available for review. Customizable Business Summary and Quality of Service dashboards provide a snapshot of factors influencing the video experience. Data points include metrics pertinent to engagement (viewers, play duration, plays abandoned, top titles, etc.) and quality (video startup time, connection speed, player startup time, etc.).

**Media Analytics – Quality of Service Monitor Module (QoS Monitor)**: To help Customer gain insight into stream health and audience engagement, QoS Monitor provides real-time visibility (by automatically refreshing every 30 seconds) into key metrics that affect the quality of video playback and viewing experience. The five key metrics tracked by default on QoS Monitor are Audience Size, Availability, Startup Time, % Rebuffering, and Bitrate.

**Media Analytics – Server-Side Analytics Module**: Server-Side Analytics enables real-time visibility for Customers that are leveraging streaming and HTTP-based delivery services for audio and video content and are unable to integrate with the media plug-in. Server-Side Analytics is available for Progressive Downloads, Flash, and Windows Media Services (WMS) streaming.

**Media Encryption**: Media Encryption is designed to help limit stream ripping attacks. This mechanism enables Edge Platform to deliver encrypted content from an edge server to the player run- time. Media Encryption provides access to customer portal to create an initial Media Encryption configuration for Adaptive Media Delivery. Customer may choose for the encryption key to be static or randomly generated to enable unique encryption per user session.

**Media Services Live (MSL)**: Media Services Live is Edge Platform's original live origin solution and includes the following capabilities:

- Accelerated ingest with UDP protocol for HLS
- Built-in redundancies for 24x7 availability and reliability
- Visibility into stream health and performance with first-mile monitoring and reporting
- Support for leading video formats for content providers to flexibly reach a fragmented online audience
- Support for RTMP ingest and stream packaging

**Media Services Live 4 (MSL 4)**: Purpose-built liveOrigin™ capabilities of Media Services Live 4 help bridge the quality and latency gap between broadcast and live streaming. Composed of ingest and mid- tier functionality, Media Services Live 4 is EDS's next generation live streaming solution specifically designed to bring the experience of broadcast TV online reliably and at scale with liveOrigin™ capabilities:

- Accelerated ingest with UDP protocol for HLS
- Minimized delays in viewing with standard end-to-end hand-wave latency of 10 seconds and ultra-low latency of 2-3 seconds
- Built-in redundancies for 24x7 availability and reliability
- Secure transport of content with end-to-end TLS
- Visibility into stream health and performance with first-mile monitoring and reporting - Bringing the TV experience online with DVR, archive and live clipping functionalities
- Support for leading video formats for content providers to flexibly reach a fragmented online audience

Media Services Live 4 also supports a modular architecture that splits ingest and origination from delivery and allows full supportability and immediate access to key Adaptive Media Delivery features.

Billing for Media Services Live 4 is based on either minutes ingested or GB ingested, and Customer elects which unit of measure shall be used when ordering Media Services Live 4.

*RTMP Ingest and Stream Packaging are only supported with MSL 3.

**Mobile Application Performance Software Development Kit (MAP SDK)**: The MAP SDK is an end-to-end architecture that utilizes Edge Platform and software to help improve performance of content on mobile devices.

**Mobile Detection and Redirect Service**: The Mobile Detection and Redirect Service provides mobile detection and redirect functionality. The matching mechanism to detect mobile devices is defined and updated periodically by Edge Platform.

**mPulse (i.e., mPulse Enterprise and mPulse Lite)**: mPulse is a web and mobile performance analytics SaaS solution designed to track and report on user experience. This real-time solution not only provides

insight into where front-end performance bottlenecks occur, but also quantifies the impact of such issues on key business performance indicators.

**NetStorage**: NetStorage, EDS' high-performance origin storage solution, is an optimized content storage solution for Customers leveraging delivery services. A key component of EDS' portfolio of storage and delivery services, NetStorage provides persistent, geo replicated storage of digital content, including images, streaming media files, software, documents, and other digital objects. The file transfer protocol is insecure. Use of this protocol may leak both access credentials and data transmitted. Customer should not use the file transfer protocol if Customer has security, integrity or confidentiality goals.

> **NetStorage – Aspera Upload Acceleration Module**: This option accelerates file transfers directly into NetStorage faster than traditional methods, using built-in connection information for NetStorage. This unique integration with Aspera achieves throughput that is multiple times higher than traditional transfer protocols, while virtually eliminating the negative effects of distance, delay, and packet loss between Customer's upload location and the NetStorage location. The resulting performance improvement dramatically reduces the time required to make content - especially time-sensitive content, high quality video files, and large content libraries - available for delivery to users across the globe via EDS' global platform.
>
> **NetStorage Ireland**: NetStorage Ireland allows one of the two standard NetStorage origin replicas, for a Customer, to be pinned specifically within the NetStorage region located in Ireland such that its content will not be moved out of country.

**Object Delivery (Media Delivery Solutions)**: This Service includes high-quality static embedded object delivery from the Edge Platform. It is designed to deliver static embedded objects under 100MB such as images, JavaScript, CSS, PDF documents, XML, and other executables over HTTP. It improves the availability and delivery performance for objects, while offering configuration options for cacheability and other services to help offload Customer's origin infrastructure.

**Origin Access Control (OAC)**: OAC is a feature of the IPA/SXL network that provides a list of gateway exit points to origin servers. The OAC ACL consists of IP addresses drawn from logical and/or physical regions that are close to the origin server. From that group, 3-6 regions are selected and 16 virtual IP addresses from each chosen region are then used to populate the OAC ACL. IP addresses on the OAC ACL are applied to an organization's firewall rules by Customer for incoming client requests (ingress). The OAC ACL is updated by Professional Services on a semi-annual basis through an email notification and a Customer acknowledgement mechanism. Origin Access Control may be seen to be complementary to the Client Access Control feature which controls client connections (egress) to the IPA/SXL system. When the IPA/SXL network detects a faster path for client requests it maps the request directly through to the origin bypassing the IPA/SXL network. As such, the OAC ACL can be used to determine if a connection came from the Edge Platform network but should not be used to block IP addresses not in the list.

**OTA Updates**: OTA Updates supports connected vehicle OEMs, IoT device and equipment manufacturers, and software developers by providing a scalable network infrastructure layer to deploy and maintain their technology. OTA Updates can reduce the number of supported versions in the field, quickly provide critical security updates, and distribute new capabilities to improve products. Remote, over-the-air software updates must be executed in a secure, trackable manner that reduces costs and time over manual deployment efforts.

**Page Integrity Manager**: Page Integrity Manager is designed to detect suspicious and malicious JavaScript behavior by instrumenting real-user sessions.

**Player Verification**: Provided as part of Media Encryption, Player Verification is designed to assist with limiting deep linking attacks by helping to ensure only an approved player is used to play HDS content.

**Premium Reporting**: Premium Reporting provides metrics and reporting on content, streams, downloads, and visitors. The specific reporting is based on the applicable Service.

**Progressive Media Downloads**: Progressive Media Downloads is designed to facilitate optimized delivery of audio and video content, thereby providing an intuitive, quality, progressive play experience. Dynamic rate limiting avoids wasted bandwidth by keeping download rates in line with the playback rate.

**Prolexic On-Prem**: Prolexic On-Prem is an on-premises service solution, powered by Corero, that is designed to protect a Customer's Protected Network from DDoS attacks. Prolexic On-Prem solution components, available in hardware or software appliances, are deployed inside the Customer's network to locally detect, mitigate and protect again DDoS attacks. Subscribers to Prolexic On-Prem service receive entitlements to hardware, software, support and maintenance necessary to deliver the service.

**Prolexic Security Solutions**: Prolexic Security Solutions are cloud-based network protection services designed to protect a designated Site from common DDoS attack vectors. It intercepts incoming traffic, inspects it for anomalies that might be consistent with DDoS attacks, and mitigates the attacks. There are three (3) versions available, and each version comes as either an Always-On service or as an On- Demand service.

The following terms refer to whether Customer's traffic will normally route through the Prolexic platform, or only route through the platform during a DDoS threat or event. The applicable Transaction Document specifies whether Customer's chosen Prolexic Service is Always-On or On-Demand.

Customer must adhere to the following GRE Requirements for the Prolexic Routed Service:

- Customer must terminate GRE on a dedicated router that supports RFC 1701, 2784.
- Must support GRE keep-alives.
- Each dedicated router must have a publicly reachable IP address to terminate the GRE tunnels.
- Support for TCP MSS adjustment: 1436 MSS (edge routers) and 1380 MSS (VPN concentrators)
- Clean, non-DDoS, inbound traffic must be less than the contracted CIR (95th percentile) for each provisioned Customer data center location, unless otherwise approved by Kyndryl.
- All dedicated routers in locations with CIR greater than 300 Mbps must support a minimum of 10Mpps with IMIX traffic.
- All dedicated routers in locations with CIR greater than 600 Mbps must have 10Gbps burstable connections to upstream transit providers, unless otherwise approved by Kyndryl.
- All dedicated routers must be capable of decapsulating GRE traffic at a rate that is at least twice the data center location CIR.

Customer is responsible for all issues related to (i) the end-to-end transit of encapsulated traffic from the Prolexic scrubbing environment to the Customer data center and (ii) the de-encapsulation of the GRE traffic at the rates received by Customer. For the On-Demand version of any Prolexic Security Solution, Customer is responsible for notifying Kyndryl when Customer's traffic must be rerouted. The exception to this is when Customer has also purchased the Flow-based Monitoring Service.

To be covered by the Prolexic Security Solutions Service Level Agreement, all implementations of the Prolexic Security Solutions must be Service Validated on an annual basis. Service Validation is a process that tests Customer's environment and service performance. In order to qualify for any Service Level Agreements applicable to Prolexic Routed, Service Validation must have been completed by Customer within the prior 12 months. Service Validations for any service may occur no more than 4 times per year.

**Prolexic Security Solution – Prolexic Protect**: Prolexic Protect is a symmetric service that is designed to protect individual Sites by directing traffic through EDS' Prolexic scrubbing centers via DNS redirection. This Service is available as always-on or on-demand, and supports protection of traffic destined for the customer origin on all ports and protocols via port forwarding.

**Prolexic Security Solution – Prolexic Routed**: Prolexic Routed is an asymmetric service that is designed to protect a Customer's Protected Network from DDoS attacks. Prolexic Routed utilizes

Border Gateway Protocol to direct traffic from Customer's network to one or more Prolexic scrubbing centers during a DDoS attack or threat of a DDoS attack. Prolexic Routed can be configured to protect all unencrypted ports and protocols.

**Prolexic Security Solution – Prolexic Routed with Connect Option**: Prolexic Routed with Connect Option is designed to provide Prolexic Routed via a direct connection from the Customer location to an EDS-designated third-party Layer2 VPN backbone or cloud service. Customer is responsible for: (i) the direct connection and Ethernet handoff to the Layer2 VPN network; (ii) contracting separately with a third party for a circuit and/or VLLs to enable delivery of Prolexic Routed with Connect Option; and (iii) the entire tail circuit, including any data center cross connects between the designated EDS connection point and Customer.

**Prolexic Security Solution - Facilitated Route-On (FRO)**: Available to On-Demand Prolexic Routed Customers, FRO allows the SOCC to review Flow-based Monitoring alerts and, as determined necessary by the SOCC and in accordance with runbook rules, initiate and conduct a BGP route change of Customer's traffic such that inbound traffic for designated network subnets will route through the Prolexic scrubbing platform without any action required by
Customer. Unless otherwise specified in writing in the customer's runbook, Kyndryl will not seek Customer's consent or otherwise notify Customer before implementing necessary BGP route changes.

**Prolexic Security Solution – Flow-Based Monitoring Service**: Flow-based Monitoring is designed to detect and alert Customer to Layer 3 and Layer 4 DDoS attacks. It uses sampled flow data obtained directly from Customer's border routers to detect DDoS attacks.

**Prolexic Security Solution – Network Cloud Firewall (NCFW)**: The Network Cloud Firewall is an integral component of the Prolexic service, and is available to Prolexic Routed, Prolexic Connect, and Prolexic IP Protect customers. This feature enforces Prolexic's zero-second SLA for any attack traffic that matches a Preconfigured Mitigation Control that is implemented within the customer- specific firewall rules. Network Cloud Firewall is designed to mitigate Layer 3 DDoS attacks and enforce traffic filtering for port and protocol-based rules. Customer-facing NCFW rules are available to customers for self-management in addition to SOCC-managed rules that will continue to be available, with each customer account being entitled to a defined number of NCFW rules in aggregate. Additional rule entitlements may be purchased for an additional fee.

**Protocol Downgrade**: Protocol Downgrade allows an HTTPS connection from the client to go forward to the origin using HTTP. The EDS network terminates the HTTPS connection.

**Rate Limiting**: Rate Limiting is designed to throttle the download rate of a file based on a setting chosen by Customer.

**REST APIs**: The REST APIs allow for stream configuration, archive and security management for Media Services Live.

**Rigor Digital Performance Monitoring**: This digital performance monitoring platform is provided via Rigor, Inc. (Rigor) and pairs synthetic monitoring technology with automated performance analysis to provide continuous visibility of the end user experience. The solution is designed to identify and provide remediation for front-end performance bottlenecks at any stage of the development process in order to prevent users from being impacted by poor performance. Certain non-EDS, non-Rigor performance programs and tools may be made available to Customer (for use with Rigor Digital Performance Monitoring) via Rigor's site labs.rigor.com or a succeeding repository. Such programs and tools are neither controlled nor provided by Kyndryl. The following support parameters apply to Customer's use of Rigor Digital Performance Monitoring, and the support parameters are subject to standard prioritization and engineering consideration to determine user impacting issues:

- Rigor shall provide chat and email support during business hours with telephone and screen share by request on a per issue basis including 24×7 access to technical support bulletins and

other user support information and forums to the full extent Rigor makes such resources available to its other customers.

- Rigor shall respond to and resolve the errors defined in the table below within the following times based on the severity of the error:

| Error Classification | Severity Definition | Response Times | Resolution Times |
|---|---|---|---|
| Service Disruption | Platform is not accessible/usable, and there is not a known workaround | Proactive email sent within 2 hours of confirmed disruption. Post-mortem sent within 48 hours of resolution. | 3 days |
| Critical | Platform is accessible but some core functionality is delayed or not usable | Initial response within 4 hours during business hours; 24 hours outside of business hours | 4 weeks |
| Standard | Platform and core functionality accessible but some non-core functionality is delayed or not usable | Initial response within 24 hours during business hours | 12 weeks |

Standard business hours are Monday - Friday, 9am EST - 6pm EST. Current Median Response Times (for issues of all severity) are as follows: During business hours = 1 hour; Outside of business hours = 12 hours

**Russia CDN Secure**: Russia CDN Secure is a performance solution that allows delivery of HTTPS content within Russia from Edge Platform servers located in Russia as well as additional servers outside Russia. Without Russia CDN Secure, HTTPS content is delivered from Edge Platform servers outside Russia. Kyndryl reserves the right to limit or restrict the amount of traffic purchased for delivery via Russia CDN and/or China CDN Services. Customers using Russia CDN and/or China CDN Services shall comply with all applicable laws in Russia and/or China, including without limitation: (i) laws that address the storage of any personal information inside Russia and/or China; and (ii) registration requirements for .ru and/or .cn sites. Customer agrees to supply Kyndryl with all documentation or registration-related information (including origin IP addresses) reasonably requested by Kyndryl. Kyndryl provides no guarantee or warranty that the Russia CDN Service or China CDN Service shall be delivered from within Russia or China, respectively. Kyndryl may deliver all or part of the China CDN Service with the use of third party suppliers, which may collect their own log files.

**Security Information and Event Management (SIEM) Integration**: SIEM Integration allows Customer to capture event details generated by EDS security products and incorporate those details into third party software (i.e., Customer's chosen SIEM solutions). EDS supports a limited set of SIEM connectors as defined by Kyndryl. The SIEM connectors made available are only samples, and Kyndryl shall not be responsible for fixing, modifying, or assisting with the implementation of the connectors.

**Security Monitor**: Security Monitor provides access to dashboards and near real-time reports to monitor security-related activity via customer portal. Security Monitor aggregates data from Customer's Kona Web Application Firewall implementation and allows Customer to monitor in near real-time when it is under attack by offering visibility into the nature of the attack, the source(s) of the attack, and an indication of which resources or assets are under attack. Security Monitor provides access to data regarding attack activity, such

as the geographies from which the attack traffic originates and which defense capabilities triggered the attack declaration.

**Session Accelerator (SXL)**: SXL empowers Customer to achieve organizational agility by leveraging the Internet as a standard platform for delivering secure business applications to any user, on any device, anywhere in the world. SXL improves the performance of Customer's business applications and does not require any hardware or virtual appliance to be installed or any software changes be made to Customer's applications.

**Site Shield**: Site Shield allows Customer to restrict traffic going to the origin infrastructure through a Site Shield Map designed to provide optimized performance for Customer. The Customer can create an IP ACL at Customer's perimeter firewall to prevent all other access to the origin. The same Site Shield Map may be used to support multiple origin locations. Changing internet conditions may require Kyndryl to change the Site Shield Map used to reach Customer's origin. Customer will be provided with at least 90 days' notice of such change. Customer must update its firewall ACLs and acknowledge the change in the customer portal within the 90-day notice period. If Customer does not do so, Customer's use of the underlying delivery product will not be covered by the associated SLAs.

**Site Shield Map**: A Site Shield Map is the set of EDS points of presence that was designed to provide optimized performance for Customer. The same Site Shield Map may be used to support multiple origin locations. Points of presence that provide optimized performance will be added to the Site Shield Map each time Customer adds an origin to the Site Shield Map, and the edge network will dynamically route traffic through these new regions to maintain performance. Site Shield Maps are not supported with the China CDN Service. Changing internet conditions require EDS to change the points of presence that EDS uses to reach Customer's origin. Customer will be provided with at least 90 days' notice of such change. Customer is required to update its firewall ACLs and acknowledge the change on the customer portal. If Customer does not acknowledge such change during the 90 days prior to the change taking place, Customer's use of the underlying delivery product will not be covered by the associated performance SLA.

**SLED - Kona Site Defender**: This service bundle is designed to meet the needs of state & local governments and educational institutions. The package includes Kona Site Defender, Client Reputation, SIEM Integration module, and Edge DNS.

**SLED - Web Application Protector**: This service bundle is designed to meet the needs of state & local governments and educational institutions. The package includes Web Application Protector and Edge DNS.

**Standard Reporting**: Standard Reporting includes access to dashboards designed to help Customer understand and analyze media delivery quality and usage. It aggregates data from standard content delivery logs. Customer accesses Standard Reporting from the customer portal.

**Standard TLS**: Standard TLS delivers an HTTPS (HTTP over TLS) service designed to encrypt data in transit. It uses Customer's TLS certificates to validate the identity of the delivery server.

**Stream Packaging (Media Services Live)**: Stream Packaging is a product option of Media Services Live 3.

**Stream Packaging (Media Services On Demand)**: Stream Packaging for Media Services On Demand is a dynamic packaging service designed to convert MP4s to HLS or HDS. This service does not support all formats of video and audio. Customer must adhere to the following requirements when using Stream Packaging:

- Customer must provide videos in a compatible format.
- Kyndryl shall not be required to provide more than 50 Gbps of peak bandwidth throughput.
- Kyndryl may require that Customer make certain technical configuration changes, which may impact links, URLs, or embedded Adobe Flash, Apple iPhone, and/or Apple iPad files deployed by Customer. Kyndryl will provide Customer with reasonable advance notification of any such required changes.

**Token Authentication**: Token Authentication is designed to help limit link sharing attacks. It authorizes the user based on a token generated using a shared secret string and an individualized salt comprised of properties specific to the user.

**Web Application Protector (WAP)**: Web Application Protector improves the security posture of Customer's protected web domains by reducing the likelihood and impact of application-level and denial- of-service attacks. It does so by intercepting suspected malicious traffic in the EDS network before it reaches Customer's protected domains.

**Web Application Protector Third Party Management Access:** This option allows Customer to assign a named third party to access and manage Customer's configuration on its behalf. This option is available for the Web Application Protector and Kona Site Defender family of Services.

**WebSockets**: The WebSockets feature allows web applications utilizing WebSockets to benefit from the performance, scale, and reliability of EDS' global platform.

## PROFESSIONAL SERVICES & SUPPORT

**Professional Services**: Unless otherwise indicated, Professional Services are charged on an hourly basis at the rate set forth in the transaction document. Depending on the nature and scope of the project, a separate statement of work may be required. Except as specified in the transaction documents and herein, nothing herein is intended to grant any rights, by license or otherwise, to Kyndryl's intellectual property or intellectual property rights. Per terms of the applicable transaction document, upon completion of integration, Professional Services will alert Customer to the availability of the Service. For any Professional Service engagement, Customer shall, in a timely manner, provide technical resources to answer any technical questions that Kyndryl personnel may have regarding requirements and deliverables. Customer will be responsible for coordinating and managing any changes to its infrastructure that may be required for integration as referenced in the applicable transaction document. Customer will be responsible for conducting functional testing for all web properties referenced in the associated transaction document prior to going live on the platform. Only those web properties referenced in the associated transaction document shall be in scope for a given Professional Services engagement. Managed Integration Services are not available for web properties that require custom user client, other than standard web browsers. Unless otherwise indicated in a transaction tocument, Managed Integration Services are limited to up to 40 hours of assistance from technical professionals.

**Advanced Service and Support**: Aligned advisory expertise, professional services, and technical support to guide, enable and mitigate business risk.

Included features:

- Advanced Monthly Service Report
- Advanced Semi-Annual Service Review
- Advanced Technical Advisor
- Advanced Professional Services
- Advanced Technical Support
- 2 Seats per year in virtual, instructor-led Edge Delivery University training courses

Advanced Monthly Service Report

- Up to 1 Monthly Service Report to be presented to the Customer at the end of each month.
- Monthly Service Report Includes a Health Check review.
  - Health Check is a programmatic check to match the configuration of an implementation with recommended practices.
  - Monthly Report and Health Check will not be presented on months where a Semi- Annual Service Review is presented.
  - Monthly Report and Health Check covers up to the number of Health Check Configurations included on the Customer Order Form.
  - Monthly Service Report and associated Health Check covers up to 1000 hostnames per configuration.

Advanced Semi-Annual Service Review

- Semi-Annual Service Report to be presented to the Customer at the end of the 6 month period.
- Semi-Annual Report Includes a Plus and Advanced Health Check review
  - Advanced Health Check review is a programmatic check to match the configuration of an implementation with recommended practices.
  - Semi-Annual Report may include recommendations based on analysis of support cases and Configuration Assistance requests.

- Semi-Annual Report and Health Check covers up to the number of Health Check Configurations included on the Customer Order Form.
- Semi-Annual Service Report and associated Advanced Health Check covers up to 1000 hostnames per configuration.

Advanced Technical Advisor

- Customer access to a designated technical advisor
- Available to conduct a monthly meeting to review in-scope service reports and recommendations with Customer presentation of the Semi-Annual Service Review with service recommendations
- Available for technical advice related to recommendations made to Customer in the Monthly Reports to assist with the adoption of recommended practices
- Technical advice is limited to the equivalent of 3 business days effort per quarter and is subject to overage at the hourly Professional Services overage rate specified on the applicable Transaction Document.

Advanced Technical Support

- Access to all items included in Standard Support.
- Advanced Service Level Agreement for Initial Response Time.
  - Advanced Support engagement within 30 minutes or less for Severity 1 issues (reported through Technical Support).
  - Advanced Support engagement within 2 hours or less for Severity 2 issues.
  - Advanced Support engagement within 1 business day or less for Severity 3 issues.
- All Support Requests reported via e-mail will be considered as Severity 3.
- Includes access to a designated primary Technical Support Engineer—during Customer Business Hours –as available.
- Unlimited Support Requests for one Customer Team

Advanced Professional Services

- Named Solution Expert
  - As available during Customer Business Hours.
  - Backed up by pooled resources when not available.

Configuration Assistance

- Ongoing, professional services to assist with configuration of the covered Web Performance or Media Products listed on the applicable Customer Order Form.
  - Up to the specified hours on the Order Form per quarter
  - Upon completion of the request, Kyndryl will respond to the Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within 3 business days will be deemed by Kyndryl as verification and acceptance of resolution of the related request.
  - Advanced Configuration Assistance does not include coverage for EDS Security products
  - Work to be conducted at mutually agreed upon dates and times during Customer Business Hours

Advanced Edge Delivery University Virtual Classroom Training

- Unless otherwise noted as Training Seats on the Customer Order Form, includes 2 seats per year in Edge Delivery University Virtual Classroom Training.
- Virtual Classroom training is led by an instructor but is delivered online only

Advanced Project Management Option

- Additional Paid Service Option for Advanced Service and Support that provides an aligned project coordinator. Project Management by Professional Services requires the Project Management line item in the applicable Customer Order Form.
  - Gaps between the setup and recommended practices identified during the Monthly Service Report and Health Check will be triaged by the Initial Acceptance Test (IAT) and get scheduled to be updated.
  - Weekly Project Report
    - Up to 1 Weekly Project Report to be shared with the customer at the end of every week except the weeks when the customer is receiving the Semi-Annual Service Review or the Monthly Project Report.
  - As of February 9th, 2023, if the Project Management line item present in the applicable Customer Order Form, The included amount of Project Management services will be indicated in Customer's Agreement through contract line items for the included Professional Service hours per quarter and the applicable overage rate.

**Enhanced Support SLA**: Enhanced Support SLA includes the following in addition to all items included with Standard Support (as set forth on the applicable Transaction Document or in the Service description of the applicable Service):

- Faster Initial Response Times from the technical support team
  - 30 minutes or less for S1 issues (must be opened via phone)
  - 2 hours or less for S2 issues
  - 1 business day or less for S3 issues
    - All Support Requests reported via e-mail will be considered as S3
- Unlimited Support Requests

**Event Support – Comprehensive**: This Service offering includes all the features of Event Support Enhanced, plus the following:

- Workflow assessments and optimizations:
- Kyndryl will implement any configuration updates for risk mitigation or quality enhancement identified during the review phase
- Advanced monitoring with specialized toolsets
- Eyes on glass
- A report with event statistics and analysis, including preventive recommendations For the duration of the event, Customer will have access to a named event coordinator via Customer's negotiated communication channel.

A minimum of 21 calendar days of notice is required to ensure Event Support coverage for Customer's event. Not all features listed in the event preparation are applicable without the 21 calendar days advance notice. This package, by default, supports events up to 4 hours. For longer events, Customer can order additional event hours for an additional fee. Minimum event hours required is 4 hours. Event hours include pre-event and post-event activities performed by Kyndryl. The scope of professional service hours is limited to risk mitigation and quality enhancements of existing EDS configurations.

**Event Support – Enhanced**: This Service offering includes all the features of Event Support Essentials, plus the following:

- Infrastructure readiness planning, unit testing and health check configuration during the event preparation phase
- Monitoring of Customer's event's performance and delivery degradation check by Kyndryl
- Proactive communications and reporting of issues during the event window
- For the duration of the event, Customer will have access to a named event coordinator via the Customer negotiated communication channel.

A minimum of 14 calendar days of notice is required to ensure Event Support coverage for an event. Not all features listed in the event preparation are applicable without 14 calendar days advance notice. This package, by default, supports events up to 4 hours. For longer events, Customer can order additional event hours for an additional fee. Minimum event hours required is 2 hours. Event hours include pre- event and post-event activities performed by Kyndryl. The scope of professional service hours is limited to risk mitigation of existing EDS configurations.

**Event Support – Essentials**: A dedicated event coordinator will engage with Customer's IT team prior to the event to (i) assess business process readiness, (i) perform risk assessments, (ii) advise on risk mitigation, and (iii) advise on creation of appropriate event alerts and monitoring during the event.
Customer's staff can reach out to a named event coordinator from the Kyndryl support team to contact for expedited issue resolution.

A minimum of 7 calendar days of notice is required to ensure Event Support coverage for Customer's event. Not all features listed in the event preparation are applicable without the 7 calendar days advance notice. This package by default supports events up to 4 hours. For longer events, Customers can order additional event hours for an additional fee. Minimum event hours required is 2 hours. Event hours include pre-event and post-event activities performed by Kyndryl. A dedicated event support engineer will be on stand-by and can join the Customer communication channel within 15 minutes of contact. Risk mitigation of EDS configuration not included in the scope of this product.

**Guided Delivery Service**: Available for Customers receiving Standard Support, Enhanced Support SLA, or Named Enhanced Support Services. Includes access to one or more of the following:

- Modular Virtual Trainings:
  - Live, web-based, short-duration, and interactive, training course(s) on EDS modules and concepts
    - Trainings will be instructor-led, delivered by the members of Professional Services
      - Customer can choose from an available list of pre-defined training modules
- Quarterly Insights:
  - Quarterly reviews to provide visibility into EDS solution utilization and share best practices
- Guided Configuration Updates:
  - Ongoing configuration change guidance from Professional Service

The base price includes 1 unit of Guided Delivery Service. Each unit of Guided Delivery Service includes the following, unless otherwise specified in the Order Form or other Transaction Document:

- Up to 4 Modular Virtual Trainings per year
- Up to 4 Quarterly Insights per year
- Up to 5 engagements per quarter of Guided Configuration Update, where an engagement, in this context, is equivalent to up to one Professional Service hour
- One pass for the annual Edge Conference

**Live Event Streaming Support**: Includes all the features of Live Event Support, plus the following for live-linear media events:

- End to end testing to scope network risks
- Monitoring of EDS' media streaming system components for availability and quality
- Automated alerting for system component availability, content quality, and audience experience for the qualified workflows
- Audience experience alerting is available only for Customer provided client–side data • Monitoring reports will be delivered to Customer during the event
- A post-event summary report will be delivered to Customer.
- For the duration of the event, Customer will have access to a named media operations expert on call or via a live phone bridge.
- A minimum of 21 calendar days of notice is required to ensure coverage for an event.

**Live Event Support**: Includes all the features of On Call Event Support, plus the following:

- Kyndryl will fully manage the implementation of any configuration updates identified in the review phase
- A comprehensive post-event report that documents key traffic metrics and summarizes root cause and resolution for any issues during the event
  - For the duration of the event, Customer will have access to a named support representative on call or via a live phone bridge.
- A minimum of 21 calendar days of notice is required to ensure coverage for an event.

**Managed Security Service (MSS) 2.0:** EDS' flagship security Service for Customers seeking to offset business risk and keep their business protected 24x7. MSS is a level of service for Customers who purchase Proactive Monitoring and Alerting for Kona Site Defender and/or Bot Manager Premier and/or Page Integrity Manager and/or App & API Protector with/without Advanced Security Management.

Managed Security Service (MSS) 2.0 offers:

**Proactive Monitoring and Alerting - available only for Kona Site Defender, Bot Manager Premier and Page Integrity Manager, and App & API Protector with/without Advanced Security Management**

1. Proactive Monitoring and Alerting
    1. Proactive monitoring of designated Kona Site Defender policies.
    2. Proactive monitoring of designated Bot Manager Premier endpoints - currently restricted to 'login' endpoint type only
    3. Proactive Monitoring of designated Page Integrity configurations
    4. Proactive monitoring of designated App & API Protector with/without Advanced Security Management policies
2. Security Event Monitoring and Attack Support
    1. Security Event Monitoring provides near real-time alerting originating from available SOCC notifications.
    2. These events are received and classified by Kyndryl. Priority assignment shall be based on event classification.
3. Proactive Detection & Notification
    1. Once an event has been recognized and categorized as security relevant, Kyndryl shall create a ticket within the ticketing system.
    2. Immediate assistance is available only via phone.
    3. Kyndryl requires 2 business days to cease performance of Proactive Monitoring and Alerting before final contract expiry
    4. For Security Events identified by the Customer, the Security Event Management process begins from the time the event is reported by the Customer to SOCC.

5. For Security Events identified by Kyndryl or by the Customer, there are instances where SOCC will engage the security Professional Services team. Any time spent by the security Professional Services team will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non-attack related requests, and attack-related requests where the mitigation solution is complex or involves significant effort.

**Security Event Management**

1. Attack Support

Kyndryl security analysts will perform an analysis of the Security Event. Identified attacks will be classified, prioritized, and escalated as Kyndryl deems appropriate in accordance with the Priority classifications under Product Support for the individual EDS' Services.

2. Customers are entitled to up to 40 reactive attack support cases per year across EDS security Services by default or as defined in the Customer's Agreement with the option to purchase additional entitlements as needed.

3. Response Times

Security Operations Command Center Support Initial Response Times:

1. 30 minutes or less for Priority 1 issues (must be opened via phone)
2. 1 hour or less for Priority 2 issues
3. 1 business day for Priority 3 issues
4. All Support Requests reported via e-mail will be considered as Priority 3
5. Initial Response Times apply only to Support Requests filed against a currently contracted security Service.

4. Kyndryl security analysts will perform an analysis of the Security Event. Whether or not a Security Event is considered an attack is determined solely by Kyndryl. Identified attacks will be classified, prioritized, and escalated as Kyndryl deems appropriate in accordance with the severity classifications under Product Support for security Services

5. For Security Events identified by Customer, the Security Event Management process begins from the time the event is reported by Customer to SOCC.

6. Post Event Report

The Post Event Report provides an analysis of a Security Event after its occurrence, including actions taken and recommendations after the Security Event has been resolved. This report is sent as needed

7. For Security Events identified by Kyndryl or by the Customer, there are instances where SOCC will engage the security Professional Services team. Any time spent by the security Professional Services team will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non-attack related requests, and attack-related requests where the mitigation solution is complex or involves significant effort.

**Attack Readiness**

1. Security Health Checks

   Security health checks enable Customers to quantify their EDS Service security posture with a grade - available only for Kona Site Defender and Page Integrity Manager.
2. Technical Security Review (TSR)
   1. For additional detail, please see Paragraph 2 of "Professional Services – Security Optimization Assistance".
   2. In addition, for KSD, PIM, and AAP with ASM, the report provides a view of a Customer's security posture in relation to their KSD/AAP with/without ASM policy(ies)/PIM configuration(s)

3. Security Configuration Assistance
   Security Configuration Assistance provides on-request security configuration assistance:
   1. Security Configuration Assistance may be utilized to make configuration changes to EDS' cloud security Services currently on contract.
   2. For additional detail, please see Paragraph 3 of "Professional Services – Security Optimization Assistance".
4. Operational Readiness Drills
   1. The Operational Readiness Drill is an exercise facilitated via a scripted scenario. It is designed to ensure existing operational plans support a fast response to a Security Event.
   2. Up to 2 Operational Readiness Drills per year or as defined in the applicable Order Form

**Advisory Services**

1. Managed Security Consultant
   1. Named contact that acts as a single point of contact to manage Customer's business priorities and communications with respect to the EDS security Services on contract.
   2. Managed Security Consultant will allocate a maximum of 51 hours/quarter to addressing on his or her responsibilities for the Customer. Any overage will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form. This is not cumulative with any other Service that provides a Managed Security Consultant.
2. Monthly Solutions Report (MSR) and Customer Business Review (CBR) - available only for Kona Site Defender, Bot Manager Premier, Page Integrity Manager, and App & API Protector with/without Advanced Security Management
   1. Monthly Solutions Report is a summary of the security activity, overall security posture, professional services fulfillment, and project updates. MSR provides transparency into security operations up to once per month. MSRs will be delivered for fully integrated security Services within the scope of Service. Configurations and policies are not covered by the MSR until the integration is completed.
   2. Customer Business Review is an executive-level business review that includes such items as industry trends and Service roadmap insights. CBR highlights the value provided by the Service to the Customer's business up to once per quarter.
   3. Upon request, Kyndryl will support a remote meeting to discuss the contents of the MSR or CBR, as applicable. Customer requested amendments to the content included in an MSR or CBR may be allowed, at Kyndryl's discretion, but any time required to implement requested customizations will be recorded against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form.
3. Attack Reporting
   Periodic summaries of attack trending and guidance, and a rollup of selected attack activities observed by Kyndryl.

**Security Event Management - Change Management Process**

1. Kyndryl will not make a change to the Customer's configuration without an associated approved change ticket within the ticketing system and approval from the Customer's authorized contacts.
2. Kyndryl is not responsible for approval by the Customer's change management board as all requested changes are assumed to be approved by said board.

**Managed Security Service (MSS) 3.0:** keeps your business protected from the most sophisticated attacks 24x7 via proactive monitoring and a rapid response in the event of a cyberattack.In addition to professional services to implement changes, our expert team includes aligned security advisors who deliver actionable insight through frequent contact and regular security reports. You can focus on growing your business, unhindered by security concerns.

Managed Security Service (MSS) 3.0 offers:

1. Proactive Monitoring and Alerting
    1. Proactive monitoring of designated Kona Site Defender / AAP / AAP with ASM policies.
    2. Proactive monitoring of designated Bot Manager Premier endpoints (Endpoints must be indeny/mitigation mode for proactive monitoring).
    3. Proactive Monitoring of designated Page Integrity configurations.
2. Security Event Monitoring and Attack Support
    1. Security Event Monitoring provides near real-time alerting originating from available SOCCnotifications.
    2. These events are received and classified. Priority assignment and action shall bebased on event classification.
    3. For Security Events identified by the Customer, the Security Event Management process beginsfrom the time the event is reported by the Customer to SOCC.
3. Proactive Detection & Notification
    1. Once an event has been recognized and categorized as security relevant, Kyndryl shall create aticket within the ticketing system.
    2. In a situation where a customer notices a security event prior to Kyndryl notifying the customerand if the customer requires immediate assistance, the customer is required to call the SOCC.
    3. Kyndryl requires 2 business days to cease performance of Proactive Monitoring and Alertingbefore final contract expiry.
    4. For Security Events identified by Kyndryl or by the Customer, there are instances where SOCC will engage the security Professional Services team. Any time spent by the security Professional Services team will be charged against Professional Services Hours entitlements at the hourly ratespecified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour willbe used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non attack related requests, and attack-related requests where the mitigation solution involves significant effort and/ or product tuning.

**Security Event Management**

1. Attack Support
   Security analysts will perform an analysis of the Security Event. Identified attacks will be classified, prioritized, and escalated as appropriate in accordance with the Priority classifications under Product Support for the individual Services.
2. Customers are entitled to up to 40 reactive attack support cases per year across security Servicesby default or as defined in the Customer's Agreement with the option to purchase additional entitlements as needed.
3. Response Times
   Akamai Security Operations Command Center Support Initial Response Times:

    1. 30 minutes or less for Severity 1 issues (must be opened via phone).
    2. 1 hour or less for Severity 2 issues.
    3. 1 business day for Severity 3 issues.
    4. All Support Requests reported via portal will be considered as Severity 2.
    5. All Support Requests reported via e-mail will be considered as Severity 3.

Initial Response Times apply only to Support Requests filed against a currently contracted security

after the Security Event has been resolved. This report is sent as needed.

4. For Security Events identified by Kyndryl or by the Customer, there are instances where SOCC will engage the security Professional Services team. Any time spent by the security Professional Services team will be charged against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time sensitive non-attack related requests, and attack-related requests where the mitigation solution is complexor involves significant effort and/ or product tuning.

**Attack Readiness**

1. Security Health Checks
   Security health checks enable Customers to quantify their Service security posture with a grade - available only for Kona Site Defender/App & API Protector (with or without ASM) and Page Integrity Manager.
2. Technical Security Review (TSR)
    1. For additional detail, please see Paragraph 2 of “Professional Services – SecurityOptimization Assistance”.
    2. In addition, for KSD/App & API Protector (with or without ASM) and PIM, the report provides a view of a Customer’s security posture in relation to their KSD/APP & API Protector policies or PIM configuration(s).
3. Professional Services Assistance
   Professional Services Assistance provides on-request security configuration assistance:
    1. Professional Services Assistance may be utilized to make configuration changes to Kyndryl’s cloud security Services currently on contract.
    2. For additional detail, please see Paragraph 3 of “Professional Services – SecurityOptimization Assistance”.
4. Operation Readiness Drills
    1. The Operational Readiness Drill is an exercise facilitated via a scripted scenario. It is designed toensure existing operational plans support a fast response to a Security Event.
    2. Up to 2 Operational Readiness Drills per year

**Advisory Services**

1. Managed Security Consultant
    1. Named contact that acts as a single point of contact to manage Customer’s business prioritiesand communications with respect to the security Services on contract.
    2. Managed Security Consultant time will be charged against Professional Services Hours entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified,the rate of $350 per hour will be used). This is not cumulative with any other Service that providesa Managed Security Consultant.
2. Support Advocacy
    1. Named technical support advocate to manage escalations and improve supportability over timewith WAF/alert trend analysis.
    2. Customers are entitled to the number of Support Advocacy hours as specified in the applicableOrder Form.
3. Technical Advisory
    1. Named technical advisor for strategic initiative planning and adoption of best practices.
    2. Customers are entitled to the number of Technical Advisory hours as specified in the

applicableOrder Form.

3. Any overage will be charged against TAS entitlements at the hourly rate specified in theapplicable Order Form.

4. Monthly Solutions Report (MSR) and Customer Business Review (CBR) - available only for Kona Site Defender/App & API Protector (with or without ASM), Bot Manager Premier and Page Integrity Manager

    1. Monthly Solutions Report (when requested) is a summary of the security activity, overall securityposture, professional services fulfillment, and project updates. MSRs will be delivered for fully integrated security Services within the scope of Service. Configurations and policies are not covered by the MSR until the integration is completed. Monthly Solutions Report will not be provided in the month in which the Customer receives the Customer Business Review.
    2. Customer Business Review is an executive-level business review that includes such items as industry trends and Service roadmap insights. CBR highlights the value provided by the Service tothe Customer's business and shall be provided once per quarter.
    3. Upon request, Kyndryl will support a remote meeting to discuss the contents of the MSR or CBR,as applicable. Customer requested amendments to the content included in an MSR or CBR maybe allowed, at Kyndryl's discretion, but any time required to implement requested customizationswill be recorded against Professional Services Hours entitlements at the hourly rate specified inthe applicable Order Form. If no hourly rate is specified, the rate of $350 per hour will be used.

5. Akamai Attack Reporting
   Periodic summaries of attack trending and guidance, and a rollup of selected attack activities observed byKyndryl.

**SOCC Premium**

SOCC Premium Support Services is an add-on service to MSS (Managed Security Service) that provides a hightouch, customer specific support experience from Akamai SOCC including any of the below:

1. Named SOCC Security Architect that have customer specific context and awareness
2. SOCC Subject Matter Experts (SME) providing:
    1. Proactive Communication on alerting customers of security events and risks and upcomingmaintenance via text and/or voice message
    2. Weekly Event Status Review with the customer to review the Post Event Reports that occurred
    3. Up to two meetings per year with the customer to collaborate, exchange information, and discuss customer status
3. Expanded Security Reviews including increased collaboration, information exchange and status reviews
4. Enhanced Site Monitoring with customer specific SIEM view in SOCC Dashboard for up to 5 Prolexic Managed AAP/APP+ASM/Kona sites
5. Priority Escalation Management including Immediate SME availability and escalation path to SOCC Management.

**Off-Hour Configuration Assistance (OHCA)**

Off-Hour Configuration Assistance enables Customers to leverage experts to make configuration changes during off hours:

1. Requests for Off-Hour Configuration Assistance must be submitted to Kyndryl via a Support Caserequesting service for Off-Hour Configuration Assistance.
2. Service Level Agreement of initial acknowledgement from an expert within 60 minutes of opening

arequest outside of business hours.

3. May be fulfilled by a non-aligned or pooled resource.
4. Service is subject to the availability of resources.
5. The request will be classified by Kyndryl. Priority assignment shall be based on request classification.
6. Includes only changes that could be performed by a Customer using portal. Excludes changes to “advanced metadata”. Excludes changes to Custom Rule Metadata.
7. Kyndryl may decline any configuration change request.
8. OHCA is only available for customers with the MSS 3.0 or Premium 3.0 products. Customers with Protect & Perform packages that include only one of these (e.g., "MSS with Plus", or "SOA with Premium") can only use OHCA for work related to the Security or Web Performance/Media Delivery product that they purchased.
9. Time spent by Professional Services performing OHCA work will consume Professional ServicesHours and be subject to overage fees.

**Security Event Management - Change Management Process**

1. Kyndryl will not make a change to the Customer’s configuration without an associated approved changeticket within the ticketing system and approval from the Customer’s authorized contacts.
2. Kyndryl is not responsible for approval by the Customer’s change management board as all requestedchanges are assumed to be approved by said board.

**Edge Delivery University**

1. Unlimited Edge Delivery University seats (subject to availability) for Virtual training type only. Virtual Classroom training is led by an instructor but is delivered online only.

**mPulse Service:** Ongoing services package aimed to provide expert assistance to optimize the usage of mPulse. It is available for customers who have purchased mPulse and includes the following features:

- mPulse Monthly Tuning Report
- mPulse Business Assessment
- mPulse Professional Services

**mPulse Monthly Tuning Report**

- Up to 1 Monthly Tuning Report to be delivered to Customer at the end of each month.
- Monthly Tuning Report summarizes site performance and trends shown per page group, device, and relevant Key Performance Indicator (KPI).
- The first Monthly Tuning Report can be delivered a month after the initial integration has been completed.
- Monthly Tuning Report covers up to 1 mPulse domain/application.
- The Monthly Tuning Report is prepared and presented per month to the Customer in a meeting for one domain.

**mPulse Business Assessment**

- A Professional Services led assessment that analyzes, documents, and presents findings for a specific area of focus from the Customer's website.
- To be performed at a mutually agreed upon time.
- Number of assessments: Up to the total number indicated on the applicable Order Form.

**mPulse Professional Services**

- Professional Services to perform updates to related mPulse configuration and related web delivery configurations, based on trends and recommendations identified in the Monthly Tuning Report and/or Business Assessment, for 1 mPulse domain/application.
- Up to the number of hours specified number of hours on the Order Form per quarter (default of 12 hours per quarter).
- Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the applicable Order Form.
- Configuration Assistance hours may be used for general Q&A about mPulse.
- Service does not include in person meetings at Customer's facilities by Kyndryl personnel unless otherwise indicated in an applicable Transaction Document.

**Named Enhanced Support**: Includes access to all items included in Standard Support, plus:

- Proactive Support. Up to 8 hours per month of proactive services from Customer's designated primary technical support engineer. May be allocated to services such as:
  - Customer Support Advocacy
  - Quarterly review calls
  - Monthly touch point calls
- Faster Initial Response Times from the technical support team
  - 30 minutes or less for S1 issues (must be opened via phone)
  - 2 hours or less for S2 issues
  - 1 business day or less for S3 issues
    - All Support Requests reported via e-mail will be considered as S3
- Named Enhanced Support live support availability
  - Live 24x7X365 support for S1 and/or S2 issues
  - Live support during regular business hours for S3 issues
- Unlimited Support Requests
- 2 Edge Delivery University seats per year
- Each unit of Named Enhanced Support includes above service coverage for up to 4 Sites or Applications. For a Customer subject to percentage-based pricing, the number of sites is not limited.
- Named Enhanced Support Plus Technical Advisory Service: Includes access to all items included in Named Enhanced Support, plus Technical Advisory Service.
- Named Enhanced Support Plus Aqua Service Management: Includes access to all items included in Named Enhanced Support, plus Aqua ION Service Management.
- Named Enhanced Support Plus Terra Service Management: Includes access to all items included in Named Enhanced Support, plus Terra Alta Service Management.
- Named Enhanced Support delivery is evidenced by Customer having the ability to submit Support Requests.

**On Call Event Support**: Includes access to event coordinator who will:

- Engage with Customer's IT team prior to the event to assess infrastructure and business process readiness
- Review Customer's configuration and recommend improvements
- Devise contingency plans and escalation procedures
- Advise on the creation of appropriate event alerts

During the event, Customer's staff will have access to a named representative from the Kyndryl support team to contact for expedited issue resolution. A minimum of 21 calendar days of notice is required to ensure coverage for an event.

**Plus Service and Support**: Expert assistance and support delivered to promote product adoption and account health for Customers with basic service requirements. Included features:

- Plus Monthly Service Report
- Plus Technical Support
- Plus Professional Services
- 1 seat per year in virtual, instructor-led Edge Delivery University training courses

Plus Monthly Service Report

- Up to 1 Monthly Service Report to be delivered to Customer at the end of each month.
- Monthly Service Report Includes a Plus and Advanced Health Check review, a programmatic check to match the configuration of an implementation with recommended practices.
- Monthly Service Report and Health Check covers up to the number of Health Check Configurations included on the applicable Transaction Document.
- Monthly Service Report does not include coverage for any EDS security Services (e.g., Web Application Protector)
- Monthly Service Report and associated Health Check covers up to 1,000 hostnames per configuration
- Review meetings for the Monthly Service Report are optional and not included in the default configuration. Customer may elect to use their Configuration Assistance (defined below) Hours towards review meetings if desired.

Plus Technical Support

- Access to all items included in Standard Support.
- Plus Service Level Agreement for Initial Response Time
    - Engagement within one hour or less for Severity 1 issues (reported through technical support resources).
    - Engagement within 2 hours or less for Severity 2 issues.
    - Engagement within 1 business day or less for Severity 3 issues.
    - All Support Requests reported via e-mail will be considered as Severity 3.
- Unlimited Support Requests for 1 Customer Team

Plus Professional Services

- Named Solution Expert
    - As available during Customer Business Hours.
    - Backed up by pooled resources when not available.

Configuration Assistance

- Ongoing, professional services to assist with configuration of the covered web performance or media Services listed on the applicable Transaction Document (does not include coverage for EDS cloud security Services).
- Up to the specified number of hours on the Order Form per quarter (default of 18 hours per quarter).
- Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the applicable Order Form.
- Configuration Assistance hours may be used for follow-up questions and detailed review of Plus Monthly Service Report if desired by Customer.
- Upon completion of the request, Kyndryl will respond to Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within 3 business days will be deemed by Kyndryl as verification and acceptance of resolution of the related request.
- Work to be conducted at mutually agreed upon dates and times during Customer Business Hours.

Plus Edge Delivery University Virtual Classroom Training

- Unless otherwise noted on the applicable Transaction Document, Plus Service and Support includes 1 seat per year in Edge Delivery University Virtual Classroom Training
- Virtual Classroom training is led by an instructor but is delivered online only.

**Premium 2.0 Service and Support**: Includes all of the Services in Standard Support plus:

- Premium Reactive Support
- Support Advocacy from a named technical support contact.
  - Up to the total number of hours per month indicated on the applicable Transaction Document
- Proactive Service Availability Monitoring
- Professional Services – Enterprise and Technical Advisory Service
  - Program management and ongoing professional services assistance
  - Access to a designated technical advisor for strategic initiative planning, engagement review, best practices
    - Limited to agreed-upon scope
    - Up to the total number of hours per month indicated on the applicable Transaction Document
- Unlimited Edge Delivery University training seats (subject to availability of courses)
- Up to 2 days of custom on-site training per year

- Each Premium Support 2.0 Unit includes:
  - Premium Reactive Support—for an additional Customer Team
  - ○ Support Advocacy from a named technical support contact.
    - Hours on applicable Order Form or other Transaction Document represent total Support Advocacy hours from all assigned advocates.
  - Reactive and Proactive Support for up to 10 additional Sites or Applications
- Service Delivery for Premium 2.0 Service and Support is evidenced by:
  - Delivery of Premium Support engagement guide to Customer
  - Customer ability to submit Support Requests.
  - Customer ability to submit requests related to the Professional Services – Enterprise Service package

**Premium 3.0 Service and Support**: High-touch Service and support engagement deeply rooted in Customer's day-to-day operations. Includes all of the Services in Standard Support plus:

- Premium Reactive Support with enhanced Service Level Agreement for Initial Response Time
  - Engagement within 15 minutes for Severity 1 issues (reported through telephone Support contact numbers)
    - Engagement within 1 hour for Severity 2 issues
    - Engagement within 1 business day for Severity 3 issues
    - Unlimited Support Requests for one Customer Team
    - Included hours
  - Program management and ongoing assistance by Professional Services
  - Ongoing, professional services to assist with configuration of the covered web performance or media products listed on the applicable Transaction Document (does not include coverage for EDS cloud security Services).
  - Number of hours: Up to the total number indicated on the applicable

Transaction Document. Hours in excess of the total number mentioned in the Transaction Document are subject to overage rate included in the Transaction Document.

- Support Advocacy
  - Named technical support contact to manage escalations and improve supportability over time
    - Number of hours - Up to the number of hours specified in Order Form
- Technical Advisory
  - Named technical advisor for strategic initiative planning and adoption of best practices
  - Number of hours - Up to the number of hours specified in Order Form
- Technical Business Assessments
  - A Professional Services led assessment that documents and presents findings for a specific area of a Customer's website(s)/application(s) and/or media asset delivery to be performed at a mutually agreed upon time.
    - Number of assessments: Up to the total number indicated on the applicable Transaction Document.
- Quarterly Business Review*
  - Up to 1 quarterly business report to be presented to Customer at the end of each calendar 3-month period.

  * Quarterly Business Reviews will consume Technical Advisory Hours.
- Premium Monthly Service Report* ○ Up to 1 Premium Monthly Service Report to be presented to Customer at the end of each month except the month when Customer receives the Quarterly Business Report.
  - Quarterly Business Report, Monthly Service Report and associated Health Check covers up to 1000 hostnames per configuration.

  * Premium Monthly Service Reports will consume Technical Advisory Hours.
- Weekly Project Report
  - Up to 1 Weekly Report to be reviewed with Customer at the end of every week except the weeks when Customer receives a Quarterly Business Report or a Premium Monthly Service Report.
- Health Checks
  - Ongoing service to ensure that implementations that have been enrolled are being constantly inspected for best practices
    - Kyndryl will periodically run programmatic checks to match the configuration of an implementation with established best practices.
    - Gaps identified between the setup and best practices will be triaged by the integrated account team and get scheduled to be updated.
    - If suitable, a review will be included in the Quarterly Business Review
    - The number of configurations enrolled: Up to the total number indicated on the applicable Transaction Document.
- Proactive Monitoring
  - Ongoing service to uncover potential, availability and configuration risks
    - Kyndryl proactively monitors issues on the EDS network that may affect availability of Customer's web and media content.
    - Proactive Monitoring keeps Customer informed of issues
    - Does not include monitoring for website/application performance or EDS' security Services.
    - Number of configurations enrolled: Up to the total number indicated on the applicable Transaction Document.

- Unlimited Edge Delivery University seats (subject to availability)
- Up to 2 consecutive days of custom on-site training per year
- Off-Hour Configuration Assistance
  - This Service enables Premium 3.0 Customers to leverage experts to make configuration changes during off hours.
- Requests for Off-Hour Configuration Assistance must be submitted via a Support Case requesting service for Off-Hour Configuration Assistance
- Service Level Agreement of initial response from an expert within 60 minutes of opening a request outside of business hours.
- May be fulfilled by a non-aligned or pooled resource.
- Service is subject to the availability of resources.
- The request will be classified by Kyndryl. Priority assignment shall be based on request classification.
- Includes only changes that could be performed by a Customer using portal
- Excludes changes to “advanced metadata” and ”EDS” cloud security Services.
- Kyndryl may decline any configuration change request
- OHCA is only available for customers with Premium 3.0 products. Customers with Protect & Perform packages that include Premium 3.0, can only use OHCA related to the Web Performance/Media Delivery products that they purchased.
- Time spent by Professional performing OHCA work will consume PS Hours and will be subject to overage fees.

**Professional Services – Edge Delivery University**: Edge Delivery University provides instructor-led training courses and training delivered by Professional Services members. Each purchased unit is equal to 1 one-time seat and can be used to attend training instances.

**Professional Services – Emergency Integration**: An additional emergency integration fee may be applied to either a Standard or Managed Integration if all or part of the integration must be completed with less than 10 business days’ notice. In order to accommodate timelines, the integration may be split into two tracks, with components requiring expedited implementation done separately from other components. Emergency integrations are subject to resource availability, and integration scope and timing must be reviewed and approved by Professional Services on a case by case basis.

**Professional Services – Enterprise**: This Service enables Customer to purchase (non-security) Professional Services for its one-off, ad-hoc custom requirements. All orders require a statement of work that details the terms and scope of the engagement.

**Professional Services – Managed Integration**: Includes Standard Integration Service plus one or more of the following project management deliverables related to the implementation and consumption of Services:

- Total project ownership and schedule
- Requirements gathering and analysis
- Implementation plan specific to Customer
- Change management process definition
- Configuration test plan
- Full life cycle project management and status reporting
- Deployment plan
- Risk assessment
- Support for go-live and associated monitoring
- Post implementation review

Off-hours support must be requested at least 10 business days in advance, at which point Kyndryl will determine if the request can be accommodated and whether additional fees are required.

### Professional Services – Managed Kona Site Defender Service

The Managed Kona Site Defender Service is an optional managed website security service for Kona Site Defender consisting of Management and Monitoring of the Kona Site Defender ("KSD" hereafter) Service with support for DDoS and Application attacks. Managed KSD Service is provided with a base configuration supporting up to 5 Protection Policies.

The base unit of Managed KSD Service includes:

- Managed KSD Service -- Attack readiness
  - Up to 25 hours Security Configuration Assistance per quarter.
  - Up to 5 Technical Security Reviews per year
  - Up to 2 Operational Readiness Drills per year
- Managed KSD Service -- Security Event Monitoring
- Managed Security Consultant - Security Event Management
- Managed KSD Service -- Security Activity Reporting
  - Post Event Report (PER)
  - Monthly Security Review (MSR)

An incremental monthly service fee is charged for each additional:

- WAF policy (beyond the base entitlement of 5) Coverage for each additional Protection Policy includes:

· + 5 hours Security Configuration Assistance per quarter, · + 1 Technical Security Review per year.

- Monitoring and Attack Support for additional Protection Policies

Managed KSD Service – Technical Security Review:

Technical Security Review includes analysis of security activities associated with 1 Protection Policy and its protected sites and/or applications as well as recommendations for security posture improvements derived from that analysis. Recommendations can be implemented as updates to the corresponding security configuration using Security Configuration Assistance hours.

Managed KSD Service – Security Configuration Assistance provides on-request security configuration assistance for Kona Site Defender.

- Security Configuration Assistance Requests must be made with at least 24 hours written notice to the Security Services Primary.
- Kyndryl will respond to all requests by the following business day. The response will include an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or alternatively, with follow-up questions to clarify the request. Upon completion of the request, Kyndryl will respond to Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within 3 business days will be deemed by Kyndryl as verification and acceptance of resolution of the related request.

Managed KSD Service – Security Event Monitoring Includes

- Security Event Monitoring provides near real-time alerting originating from available KSD notifications.
- These events shall be received and classified by Kyndryl. Event classification shall result in the assignment of a priority to each individual log event. Events classified with priority 1, 2, or 3 are considered security relevant events requiring further analysis and/or escalation to a Customer authorized contact.

- Once an event has been recognized and categorized as security relevant, Kyndryl's monitoring system shall open a ticket within the ticketing system corresponding to the Security Incident. This ticket shall be analyzed by security response staff and escalated to the Customer's authorized contact if it is not possible to classify the incident as a false positive.

Managed KSD -- Security Event Management Includes:

- Security Operations Command Center Support Initial Response Times:
  - 30 minutes or less for Priority 1 issues (must be opened via phone)
  - 1 hour or less for Priority 2 issues
  - One Business Day for Priority 3 issues
  - All Support Requests reported via e-mail will be considered as Priority 3
  - Managed Kona Site Defender Initial Response Times apply only to Support Requests filed against the Kona Site Defender product.
- Immediate assistance is available only via phone
- Kyndryl security analysts will perform an analysis of the Security Event. Identified attacks will be classified, prioritized, and escalated as Kyndryl deems appropriate in accordance with the Priority classifications under Product Support for Kona Products
- The Attack Support detailed priority descriptions, level of support, and SLAs are specified in the applicable Service's customer engagement guide (e.g., Managed Kona Site Defender Service Customer Engagement Guide).
- For Security Events identified by the Customer, the Security Event Management process begins from the time the event is reported by the customer to SOCC.

Security Event Management -- Change Management Process

- Kyndryl will not make a change to the Customer's configuration without an associated approved change ticket within the ticketing system and approval from the Customer's authorized contacts.
- Kyndryl is not responsible for approval by the Customer's change management board, as all requested changes are assumed to be approved by said board.

**Professional Services – Readiness and Response Service (RRS):** Prioritized access to security experts for advisory support and direct access to SOCC for reactive support for the EDS security Services on contract. RRS is a level of service including access to one of more of the following:

1. Technical Security Reviews (TSR):
   1.1. For additional detail, please see Section 2 of "Professional Services – Security Optimization Assistance" description.

2. Security Configuration Assistance:
   2.1. For additional detail, please see Paragraph 3 of "Professional Services – Security Optimization Assistance" description.

3. Security Event Management:
   3.1. 24x7 reactive support for Security Events related to the EDS security Services on contract
   3.2. Customers are entitled up to 40 reactive attack support cases per year across EDS security Services by default or as defined in the Customer's Agreement with the option to purchase additional entitlements as needed.
   3.3. Security Operations Support Initial Response Times:
      3.3.1. 30 minutes or less for Severity 1 issues (must be opened via phone)

3.3.2. 1 hour or less for Severity 2 issues
3.3.3. 1 Business Day for Severity 3 issues
3.3.4. All Support Requests reported via email will be considered as Severity 3
3.3.5. Security Operations Support Initial Response Times apply only to Support Requests filed against a currently contracted security Service.

3.4. Security analysts will perform an analysis of the Security Event. Whether or not a Security Event is considered an attack is determined solely by Kyndryl. Identified attacks will be classified, prioritized, and escalated as Kyndryl deems appropriate in accordance with the severity classifications under Product Support for EDS security Services

3.5. For Security Events identified by Customer, the Security Event Management process begins from the time the event is reported by Customer to SOCC.

**Advisory Services**

4. Managed Security Consultant

4.1. Named contact that acts as a single point of contact to manage Customer's business priorities and communications with respect to the EDS security Services on contract.

4.2. Managed Security Consultant will allocate a maximum of 20 hours/quarter to addressing on his or her responsibilities for the Customer. Any overage will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form. This is not cumulative with any other Service that provides a Managed Security Consultant.

5. Additional Terms

5.1. Readiness and Response Service does not include assistance related to the use of EDS security Services for any purpose not stated in the service description of the contracted Service(s) consumed by the Customer.

5.2. Security Event Management is limited to the capabilities of the supported Service.

5.3. Security Event Management for Bot Manager does not provide defense against direct to origin attacks.

5.4. For Security Events identified by Kyndryl or by the Customer, there are instances where SOCC will engage the Security Professional Services team. Any time spent by the Security Professional Services team will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form. The scope of work for which the Security Professional Services team is engaged includes, but is not limited to, time-sensitive non-attack related requests, and attack-related requests where the mitigation solution is complex or involves significant effort.

5.5. Readiness and Response service is a Customer-initiated support service and does not include Security Event monitoring or proactive support for Security Events.

5.6. Service does not include the initial integration of the security Services, nor does it include the implementation of the Service to cover additional properties. Any such implementation requires a separate fee.

**Professional Services – Security**: Includes access to Professional Services for assistance with EDS security Services. The term and scope of the engagement will be defined in an applicable statement of work.

**Professional Services – Security Optimization Assistance (SOA):** Expert assistance to optimize and maintain the EDS security Services on contract. SOA is a level of service including access to one or more of the following:

1. Named Security Expert:

1.1. A designated security expert aligned with the Customer's team

1.2. This expert coordinates Customer's Security Optimization Assistance deliverables, works closely with Customer's team to understand Customer's security profile and business priorities, provides contextual recommendations and also coordinates the implementation of changes to Customer's security configurations when required

2. Technical Security Reviews (TSR):
   2.1. Technical Security Review is an on-demand deliverable based on entitlements. The objective of the report is to present an analysis and to provide actionable recommendations.
   2.2. One Technical Security Review will include the review of only one of the covered security Services and the detailed scope per Service is defined in 2.9. - 2.17.
   2.3. A Technical Security Review for enterprise security Services (Enterprise Threat Protector/Enterprise Application Access/Enterprise Defender) requires the enterprise security coverage line item. The maximum number delivered per year is defined on the enterprise security coverage line item in the applicable Order Form.
   2.4. Technical Security Reviews do not include implementation of specific configuration recommendations. Those may be implemented using Security Configuration Assistance hours or may be implemented by Customer.
   2.5. Upon request, Kyndryl will support a remote meeting to discuss the contents of the TSR. Customer requested amendments to the content included in a TSR may be allowed, at Kyndryl 's discretion, but any time required to implement requested customizations will be recorded against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form.
   2.6. Customers are entitled to receive up to the number of Technical Security Reviews per year as included on the applicable Order Form.
   2.7. Kyndryl reserves the right to execute no more than 1/3 of the Technical Security Reviews in any single calendar quarter.
   2.8. Technical Security Reviews not consumed during the contract year will expire
   2.9. A Technical Security Review for Kona Site Defender includes:
      2.9.1. Analysis of up to 1 security policy and components with corresponding actionable recommendations
   2.10. A Technical Security Review for Prolexic Routed (or Prolexic Routed with Connect option) includes:
      2.10.1. Analysis of one location/data center
      2.10.2. Recommendations to mitigate identified issues – e.g., latency that might indicate the Customer needs to migrate to another scrubbing center for mitigation to reduce the impact.
   2.11. A Technical Security Review for Bot Manager Premier includes:
      2.11.1. Analysis of bot activity on up to 5 resource purpose names or endpoints with corresponding actionable recommendations.
   2.12. A Technical Security Review for Web Application Firewall includes:
      2.12.1. Analysis of up to 1 security policy and components with corresponding actionable recommendations
   2.13. A Technical Security Review for Page Integrity includes:
      2.13.1. Review for up to 1 Page Integrity configuration
   2.14. A Technical Security Review for Enterprise Threat Protector includes:
      2.14.1. Review of up to 1 ETP Configuration
   2.15. A Technical Security Review for Enterprise Application Access includes:
      2.15.1. Review of up to 1 EAA Configuration
   2.16. A Technical Security Review for Enterprise Defender includes:
      2.16.1. Review of one of the following: Up to 1 EAA Configuration, up to 1 ETP Configuration, or up to 1 KSD Policy covered by the Enterprise Defender package

2.17. A Technical Security Review for App & API Protector (with or without Advanced Security Management) includes:

2.17.1. Analysis of up to 1 security policy and components with corresponding actionable recommendations

2.18. A TSR for any security Service other than those listed in 2.9 - 2.17 may be allowed, at Kyndryl's discretion, but any time required to execute on the TSR will be recorded against Technical Security Review entitlements as specified in the applicable Order Form.

3. Security Configuration Assistance:

3.1. Ongoing, Security Professional Services to assist with configuration of the covered security Services

3.2. Up to the specified hours per quarter as defined on the applicable Order Form

3.3. The usage of Security Configuration Assistance for Enterprise security Services (Enterprise Threat Protector/Enterprise Application Access/Enterprise Defender) requires the enterprise security coverage line item. The maximum number of available hours per quarter is defined on the enterprise security coverage line item in the applicable Order Form.

3.4. Service does not include the initial integration of the security Service, nor does it include the implementation of the Service to cover additional properties. Any such implementation requires a separate fee.

3.5. Security Configuration Assistance in excess of the available quarterly hours will be billable at the overage rate included on the applicable Order Form. If no overage rate is specified, the rate of $350 per hour will be used.

3.6. Security Configuration Assistance Requests must be made with at least 1 full business day written notice to the security Services team.

3.7. Kyndryl will respond to all requests by the following business day providing either (i) an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or (ii) follow-up questions to clarify the request.

3.8. Upon completion of the request, Kyndryl will respond to the Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within 3 business days will be deemed by Kyndryl as verification and acceptance of resolution of the related request.

4. Additional Terms:

4.1. Security Optimization Assistance does not include assistance related to the use of EDS security Services for any purpose not stated in the service description of the supported Services purchased by Customer

4.2. Technical Security Reviews do not include implementation of specific configuration recommendations. Those may be implemented using Security Configuration Assistance hours or may be implemented by Customer.

4.3. Security Configuration Assistance is not intended to provide Attack Support

**Professional Services – Service Management 2.0**: Includes access to one or more of the following:

- Named Solution Expert
- Quarterly Optimization Schedule: Scheduled technical review of existing EDS configurations and recommendations for improvement managed by Kyndryl. Each Quarterly Optimization Schedule covers 1 configuration and 1 site. Customer can purchase Optimization Schedules for up to the number of configurations specified on the applicable Transaction Document (the default is 2 configurations).
- Up to the number of hours per quarter specified on the applicable Transaction Document (the default is 18 hours per quarter) of ongoing Professional Services to perform updates to existing EDS configurations. Any configuration change will be performed using Professional Services hours.

**Professional Services – Standard Integration**: Includes activation of the applicable Service as set forth on the associated Transaction Document. This may include any or none of the following:

- Telephone support to (i) conduct a training session for online tools for configuration management, reporting, and troubleshooting, and (ii) answer specific implementation questions
- E-mail and/or web conferencing support to assist Customer with the activation process
- Standard Integration Services are provided at mutually agreed upon dates and times during normal business hours (i.e., 9:00 am to 5:00 pm Customer local time).
- Unless otherwise indicated in an applicable Transaction Document, Standard Integrations are limited to up to 8 hours of assistance from an integration specialist and/or other EDS professionals.

**Protect and Perform**: Protect and Perform service bundles combine Service and Support packages for Security with Web Performance/Media Delivery (core) service packages. Each Protect & Perform bundle includes one Security service package and one core service package. There are three Security Services available in the Protect and Perform bundles:

- Managed Security Service -- (MSS)
- Readiness and Response Service -- (RRS)
- Security Optimization Assistance -- (SOA)

There are three Web Performance/Media Delivery (core) Services available in these bundles:

- Premium 3.0 Service and Support – (Premium)
- Advanced Service and Support – (Advanced)
- Plus Service and Support -- (Plus)

The shorter names for each of these Services (in parenthesis) identify each of the two Services included in a bundle. Except for the enhancement of Shared PS Hours, product entitlements included in the bundle are functionally identical to the entitlements described in this document under the full Service names listed above.

The following Protect and Perform bundles are currently offered:

- Protect & Perform MSS with Premium
- Protect & Perform MSS with Advanced
- Protect & Perform MSS with Plus
- Protect & Perform RRS with Premium
- Protect & Perform RRS with Advanced
- Protect & Perform RRS with Plus
- Protect & Perform SOA with Premium
- Protect & Perform SOA with Advanced
- Protect & Perform SOA with Plus
- Protect & Perform – Shared PS Hours:

Protect and Perform bundles offer the feature of Shared PS Hours. Shared PS Hours are a quarterly allocation of Professional Services Hours that may be used for Configuration Assistance for both EDS security and web/media Services.

The following deliverables are available through an additional quarterly allocation of hours as indicated via separate line items on the Customer's applicable Transaction Document(s). Shared PS Hours may not be used for any of these deliverables:

- Technical Advisory Services for Advanced

- Project Management for Advanced
- Technical Advisory Services for Premium
- Support Advocacy Services for Premium
- Project Management for Advanced

**Standard Support**: Standard Support is EDS base level technical support. Standard Support includes access to all of the following:

- Self-service configuration tools
- Pooled technical support account team
- Standard Support Initial Response Times
    - 2 hours or less for Severity 1 issues
    - 4 hours or less for Severity 2 issues
    - 2 business days or less for Severity 3 issues
    - All Support Requests reported via e-mail will be considered as Severity 3
    - Live support during Customer Business Hours for Severity 2 and/or Severity 3 issues
- Live 24x7X365 support for Severity 1 issues
- Up to 15 Support Requests per year across all EDS Services
- Included with all EDS Services for direct Customers unless otherwise set forth on the applicable Transaction Document or in the Service description of the applicable Service.

**Technical Advisory Service**: Includes access to a designated technical advisor during Customer Business Hours, up to an agreed upon number of hours or Business Days (specified on the associated Transaction Document), for advisory services that can include any one or more of the following activities:

- Provide pre- and post-sales technical consultation
- Assist with strategic initiatives through ongoing engagement
- Schedule periodic status meetings
- Conduct periodic engagement reviews
- Share industry and technology best practices with Customer
- For travel to Customer's premises, Customer shall be responsible for reasonable additional fees for travel and living related expenses for Kyndryl's technical team.

# Service Level Agreements (SLA)

## Service Level Agreement for Dynamic Site Accelerator (DSA)

### I. Service Levels

Kyndryl agrees to provide a level of service per the terms below:

(1) Improvement Over Origin: The daily average page delivery time using the DSA service will be at least 50% faster than the daily average delivery time for the same page delivered from the customer's origin server (defined as the daily average page delivery time from origin being at least 1.5 times the daily average page delivery time using the DSA service).

(2) 100% Availability: The Service will serve content 100% of the time.

### II. SLA Monitoring Methodology

#### A. Performance SLA Monitoring Methodology

The following methodology will be employed to measure the performance improvement provided by the Service:

(1) A single static unauthenticated page (including HTML and associated embedded content), selected and agreed upon by Kyndryl and Customer, will be tested throughout the term of the DSA Order Form for purposes of this SLA. Kyndryl will make a sample static page (including HTML and associated embedded content) available for use by customers.

(2) Delivery times will be tested using Site Analyzer testing services to measure the daily average page delivery time computed from the complete global set of available Site Analyzer measurement agents. The tests will be configured to take place once an hour from the measurement agents.

(3) This SLA assumes that there will be no material changes to the test content including, without limitation, metadata applied to the content, agent network used for testing, origin settings and origin infrastructure; any such changes will nullify a deficient test result.

(4) This SLA shall not apply if there is limited or no performance improvement due to causes originating from customer's infrastructure or a third party's infrastructure outside of Kyndryl's control, including the customer's DNS that provides the CNAME into the EDS network. Kyndryl reserves the right to remove DNS times from the speedup computation if deemed necessary.

#### B. Availability SLA Monitoring Methodology

The following methodology will be employed to measure the Service availability:

*Agents and Polling Frequency*

(1) From at least six (6) geographically and network-diverse locations in major metropolitan areas, Kyndryl will simultaneously poll a test file residing on the Customer's production servers and on EDS network

(2) The polling mechanism will perform two (2) simultaneous http GET operations:

A test file will be placed on the customer's origin server (i.e., origin.customer.com).

One GET operation will be performed to retrieve the file directly from the origin server (i.e., http://origin.customer.com/testobject).

The other GET operation will be performed to retrieve the file through the Service, by requesting the object from the appropriate customer hostname CNAMEd to EDS (i.e., http://www.customer.com/testobject, where

www.customer.com is CNAMEd to EDS and configured to pull content from origin.customer.com)

(3) The test content must use a TTL of 2 hours or greater.

(4) The test content will be a file of approximately 10 KB in size.

(5) Polling will occur at approximately 6-minute intervals.

(6) Based on the http GET operations described in II-B above, the response times received from the two sources, (a) the Customer server (directly), and (b) the EDS network, will be compared for the purpose of measuring performance metrics and outages.

**III. Outage**

An availability outage is defined as a period of at least two consecutive failed attempts six minutes apart by a single agent to GET the Customer test file from the Service while succeeding to GET the test file from the Customer Origin Server (directly).

**IV. SLA Activation**

**A. Performance SLA Activation**

To activate this SLA, Customer and Kyndryl will designate the applicable page as contemplated by II-A (1) above. Customer shall be responsible for configuring such page to enable testing by the measurement agents. Customer shall be responsible for configuring the Site Analyzer service for measurement of the designated page.

**B. Availability SLA Activation**

In order to activate the Service Level Agreement, the Customer must enter and indicate the location of two valid test files for the same object (as described in II(B) above) into the SLA Activation Tool located in the Customer Portal. Detailed instructions are provided with the SLA Activation Tool; in addition, assistance is available from the Customer's Account Manager. The SLA will go into effect within five business days after the Customer enters valid test files into the SLA Activation Tool.

**V. SLA Escalation**

In order to request a credit for a perceived service failure, Customer must, within five calendar days (120 hours) after the perceived failure, contact Kyndryl in specifying the time period in which the failure is believed to have occurred.

**VI. Remedies**

If the Service fails to meet the service levels in Section I or if an Outage, as defined in Section III, is identified, the Customer will receive (as its sole remedy) a credit equal to Customer's committed monthly service fee for the day in which the failure occurs, not to exceed 30 days of fees.

## Service Level Agreement for Enterprise Application Access – Essentials and Enterprise option

**I. Service Levels and Credits**

Kyndryl agrees to provide a level of service demonstrating:

(a) 100% Uptime: The Enterprise Application Access (EAA) Service will have no Outages (as defined below).

(b) Credits: If the EAA Service fails to meet the above service level, the Customer will receive (as its sole

remedy) a credit equal to EAA fees for the day in which the failure occurs, not to exceed thirty (30) days of fees in any monthly billing period. Multiple Outages in the same calendar day will constitute one SLA failure for purposes of calculating the credits owed.

## II. SLA Monitoring Methodology

The following methodology will be employed to measure EAA Service availability:

*Polling Targets*

For each EDS Cloud Zone (ACZ), Kyndryl will configure an SLA application and corresponding unique hostname that will be hosted at the ACZ. This "SLA hostname" is used as the polling target for measuring EAA service availability.

*Agents and Polling Frequency*

For each ACZ used by the Customer, Kyndryl will:

(a) Poll the SLA hostname from six (6) network-diverse locations (i.e., agents) within 150 ms of the ACZ. Over a six-minute polling period, each agent polls the SLA hostname once in round-robin format with approximately a 60-second gap between agent polls.

(b) The polling mechanism will perform an HTTP GET operation on the SLA hostname. Success of an HTTP GET is defined as a reply being received from the target SLA hostname with a 200 or 300 HTTP status code.

(c) Each polling period will occur at approximately 12-minute intervals.

(d) Based on the HTTP GET operation described in II(b) above, the response will be assessed for the purpose of measuring Outages.

## III. Outages

An "Outage" of a single ACZ is defined when all six (6) agents are unsuccessful in performing an HTTP GET operation of the ACZ's SLA hostname during a polling period. If any ACZ used by the Customer has an Outage, the EAA Service has an Outage.

## IV. Credit Request

In order to receive a credit, the Customer must contact Kyndryl and formally declare an Outage. Kyndryl will determine, in its sole discretion based upon the above methodology, whether an SLA failure has occurred and any applicable credit amount.

Credits will be available as credits to invoices only and will be applied to the invoice for the next billing period following the period for which the Outage occurred.

## V. Exclusions

The SLA applies only to the EAA Service and does not apply to the following: a) planned downtimes during upgrades or other maintenance, b) free Services, including without limitation free Service features and options (e.g., Services, features, and/or options provided during technical preview, beta, introductory trial, or evaluation periods), or c) Outages caused by factors outside Kyndryl's reasonable control or use of the Service other than as explicitly permitted by the relevant service agreement terms.

## Service Level Agreement for Edge DNS

### 1. Definitions

a. Customer - An organization with a current EDS Account.
b. Methodology - A valid testing methodology must meet the following requirements:
   i. A minimum of five (5) testing agents using a recursive resolver in diverse geographic and network locations. The resolver must utilize standard delegation retry configuration that follows delegation chains and attempts authoritative queries against multiple delegations.
   ii. Each testing agent must have a polling frequency of five (5) minutes or less.
   iii. Test results must be able to demonstrate whether each testing agent could resolve the root DNS servers for the DNS zone (e.g., .com, .net, .gov) in addition to whether the testing agent could resolve an Edge DNS zone.
   iv. Any changes to zone record data must propagate for at least 15 minutes before testing of that record begins.
c. Zone Delegation Configuration - For a valid Service Level Commitment, a customer must list with its registrar all EDS nameserver delegations for the Edge DNS contract and configure those nameserver delegations in their zone's data.
d. Successful Resolution - A NOERROR response for a configured record in a customer domain or an NXDOMAIN response for a nonexistent record in a customer domain.
e. Outage - Failed attempts to resolve a DNS record registered with zone data from multiple networks for at least five (5) minutes while resolutions for the root DNS servers for the zone succeed.
f. Uptime - The percentage of time the service provides an expected DNS response, as measured with a valid testing Methodology.

### 2. Service Level Commitment

Kyndryl agrees to provide a level of service demonstrating 100% Uptime, as measured with a valid testing Methodology.

### 3. Credits

For failure to meet applicable Service Level Commitment, Kyndryl shall provide a Credit equal to fees for the day in which the Outage occurs, not to exceed 30 days of fees.

### 4. Procedures

To be eligible for Credits, Customer must submit written notice to Kyndryl at the time observing the problem and send a request, within five (5) calendar days after the perceived service Outage, to Kyndryl for service Credits with recent, relevant details (i.e., data from tests using a valid Methodology) sufficient for Kyndryl to validate the request. Upon validation, Kyndryl shall apply the appropriate Credit to the Customer's account. Credits shall be applied to invoices for payment periods subsequent to the current or previous period in which the SLA failure giving rise to the Credit(s) occurred only. In no event shall Kyndryl provide refunds or cash payments of Credits. A Customer must be current in its payments in order for service Credits to be applied to its account.

### 5. Monitoring Report

The Customer Portal provides a service availability report to help follow Uptime.

## Service Level Agreement for Enterpriser Threat Protector

### I. Service Levels and Credits

Kyndryl agrees to provide a level of service demonstrating:

(a) 100% Uptime: Every client request through the Enterprise Threat Protector (ETP) service will be directed to a live Customer server 100% of the time.

(b) Credits: If the Enterprise Threat Protector service fails to meet the above service level, the Customerwill receive (as its sole remedy) a credit equal to fees for the day in which the failure occurs

II. **SLA Monitoring Methodology**

The following methodology will be employed to measure Enterprise Threat Protector service availability:

Agents and Polling Frequency

(a) Customer may perform a service availability test by performing DNS lookups or HTTP requests from at least five (5) geographically and network-diverse locations in major metropolitan areas. Availability testing occurs at acustomer-specified frequency of not to exceed one request every five (5) minutes per testing agent.

(b) DNS Tests should be performed against a valid internet hostname and DNS record type that is specified as part of the customer's configuration. This hostname will be pre-cached by the ETP service to eliminate failuresdue to authoritative DNS server failures.

(c) HTTP Tests should be performed against a valid internet hostname and URL that is specified as part of thecustomer's configuration. This hostname will be set to block by the ETP service to eliminate failures due to origin server failures.

(d) One service availability hostname will be set up per customer.

III. **Outages**

An "Outage" is defined as a failed attempt by the Enterprise Threat Protector service to resolve the name of the customer's configured service availability hostname across all testing agents for a period of at least 10 minutes. If an Outage is identified by this method, the customer will receive (as its sole remedy) a credit equivalent to thefees for the day in which the outage occurred.

For any Customer using DNS Proxy with the ETP service, if the Customer implements a service configurationother than as suggested by Kyndryl, and if such configuration results in downtime of the ETP service, such downtime will not be considered an Outage and the Customer shall not be entitled to receive any credit from Kyndryl for such downtime.

IV. **Procedures**

To be eligible for Credits, Customer must submit written notice to Kyndryl at the time observing the problem and send a request, within five (5) calendar days after the perceived service Outage, to Kyndryl for service Credits with recent, relevant details (i.e., data from tests using a valid Methodology) sufficient for Kyndryl to validate the request. Upon validation, Kyndryl shall apply the appropriate Credit to the Customer's account. Credits shall be applied to invoices for payment periods subsequent to the current or previous period in which the SLA failure giving rise to the Credit(s) occurred only. In no event shall Kyndryl provide refunds or cash payments of Credits. A Customer must be current in its payments in order for service Credits to be applied to its account.

## Service Level Agreement for Ion – includes Ion, Ion Standard and Ion Premier

### I. SLA Monitoring Methodology

Kyndryl agrees to provide a level of service per the terms below:

(1) Improvement Over Origin: The daily average page delivery time using the Ion Standard service will be at least 100% faster than the daily average delivery time for the same page delivered from the customer's origin server (defined as the daily average page delivery time from origin being at least 2 times the daily average page delivery time using the Ion Standard service).
(2) 100% Availability: The Service will serve content 100% of the time.

### II. SLA Monitoring Methodology

**A. Performance SLA Monitoring Methodology**

The following methodology will be employed to measure the performance improvement provided by the Service:
(1) A single static unauthenticated page (including HTML and associated embedded content), selected and agreed upon by Kyndryl and Customer, will be tested throughout the term of the Ion Standard Order Form for purposes of this SLA. Kyndryl will make a sample static page (including HTML and associated embedded content) available for use by customers.
(2) Delivery times will be tested using Kyndryl's Site Analyzer testing services to measure the daily average page delivery time computed from the complete global set of available Site Analyzer measurement agents. The test will be configured to take place once an hour from the measurement agents.
(3) This SLA assumes that there will be no material changes to the test content including, without limitation, metadata applied to the content, agent network used for testing, origin settings and origin infrastructure; any such changes will nullify a deficient test result.
(4) This SLA measurement will not include DNS lookup times
(5) This SLA shall not apply if there is limited or no performance improvement due to causes originating from customer's infrastructure or a third party's infrastructure outside of Kyndryl's control, including the customer's DNS that provides the CNAME into the EDS network. Kyndryl reserves the right to remove DNS times from the speedup computation if deemed necessary.

**B. Availability SLA Monitoring Methodology**
The following methodology will be employed to measure the Service availability:
*Agents and Polling Frequency*
(1) From at least six (6) geographically and network-diverse locations in major metropolitan areas, Kyndryl will simultaneously poll a test file residing on the Customer's production servers and on EDS network
(2) The polling mechanism will perform two (2) simultaneous http GET operations:
A test file will be placed on the customer's origin server (i.e., origin.customer.com).
One GET operation will be performed to retrieve the file directly from the origin server (i.e., http://origin.customer.com/testobject).
The other GET operation will be performed to retrieve the file through the Service, by requesting the object from the appropriate customer hostname CNAMEd to EDS (i.e., http://www.customer.com/testobject, where www.customer.com is CNAMEd to EDS and configured to pull content from origin.customer.com)
(3) The test content must use a TTL of 2 hours or greater.
(4) The test content will be a file of approximately 10 KB in size.
(5) Polling will occur at approximately 6-minute intervals.
(6) Based on the http GET operations described in II-B above, the response times received from the two sources, (a) the Customer server (directly), and (b) the EDS network, will be compared for the purpose of measuring performance metrics and outages.

**III. Outage**
An availability outage is defined as a period of at least two consecutive failed attempts six minutes apart by a single agent to GET the Customer test file from the Service while succeeding to GET the test file from the Customer Origin Server (directly).

**IV. SLA Activation**
**A. Performance SLA Activation**
To activate this SLA, Customer and Kyndryl will designate the applicable page as contemplated by II-A (1) above. Customer shall be responsible for configuring such page to enable testing by the measurement agents. Customer shall be responsible for configuring the Site Analyzer service for measurement of the designated page.
**B. Availability SLA Activation**
In order to activate the Service Level Agreement, the Customer must enter and indicate the location of two valid test files for the same object (as described in II(B) above) into the SLA Activation Tool located in the Customer Portal. Detailed instructions are provided with the SLA Activation Tool; in addition, assistance is available from the Customer's Account Manager. The SLA will go into effect within five business days after the Customer enters valid test files into the SLA Activation Tool.

**V. SLA Escalation**

In order to request a credit for a perceived service failure, Customer must, within five calendar days (120 hours) after the perceived failure, contact Kyndryl in writing, specifying the time period in which the failure is believed to have occurred.

**VI. Remedies**

If the Service fails to meet the service levels in Section I or if an Outage, as defined in Section III, is identified, the Customer will receive (as its sole remedy) a credit equal to Customer's committed monthly service fee for the day in which the failure occurs, not to exceed 30 days of fees.

## Service Level Agreement for Global Traffic Management - Standard and Premier option

### 1. Definitions

1. Customer - An organization with a current EDS Account.
2. Methodology - A valid testing methodology must meet the following requirements: 1. A minimum of five (5) testing agents using a recursive resolver in diverse geographic and network locations. The resolver must utilize standard delegation retry configuration that follows delegation chains and attempts authoritative queries against multiple delegations.
    2. Each testing agent must have a polling frequency of five (5) minutes or less.
    3. Test results must demonstrate whether each testing agent can resolve the root DNS servers for the domain (e.g., .com, .net, .gov) in addition to whether the testing agent could resolve GTM domain and property.
    4. Any changes to the domain which affect the property must propagate for at least 15 minutes before the property is tested.
3. Successful Resolution - A NOERROR response for a configured record in a customer domain or an NXDOMAIN response for a nonexistent record in a customer domain.
4. Outage - Failed attempts to resolve a DNS query to a GTM domain and property with a registered Customer IP address or CNAME for at least five (5) minutes, while resolutions for the root DNS servers for the domain succeed.
5. Uptime - The percentage of time the service provides an expected response, as measured with a valid testing Methodology.

### 2. Service Level Commitment

Kyndryl agrees to provide a level of service demonstrating 100% Uptime, as measured with a valid testing Methodology.

### 3. Credits

For failure to meet applicable Service Level Commitment, Kyndryl shall provide a Service Level Credit equal for the day in which the Outage occurs.

### 4. Procedures

To be eligible for Credits, Customer must submit a ticket to Kyndryl at the time observing the problem and send a request, within five (5) calendar days after the perceived service Outage, to Kyndryl for service Credits with recent, relevant details (i.e., data from tests using a valid Methodology) sufficient for Kyndryl to validate the request. In no event shall Kyndryl provide refunds or cash payments of Credits. A Customer must be current in its payments in order for service Credits to be applied to its account.

### 5. Monitoring Report

The Customer Portal provides a service availability report to help follow Uptime.

## Service Level Agreement for EDS Cloud Security Solutions

## DEFINITIONS

**"Attack Monitoring Services - Failure to Notify Event"** is an event in which Kyndryl fails to take the defined steps to notify Customer within a period of 15 minutes from the time that Security Operations Center (SOC) receives a Critical alert (applicable only to Prolexic Application-Based Monitoring and Prolexic Flow Based Monitoring Services deployed at the Customer site).

"**EDS Network**" means the distributed network owned and operated by Edge Delivery Services.

"**Prolexic Network**" means the distributed network of specialized network of scrubbing centers owned and operated by Edge Delivery Services.

**"Availability Outage"** (applicable only to Kona Site Defender, Kona DDoS Defender, Web Application Protector, Web Application Firewall, Bot Manager Standard, Bot Manager Premier, and Site Shield) is defined as a period of at least two consecutive failed attempts six (6) minutes apart by a single agent to GET the Customer test file from the Service while succeeding to GET the test file from the Customer Origin Server (directly, or via a Site Shield region if applicable). If an outage is identified by this method, the Customer will receive (as its sole remedy) a credit equal to Customer's or such domain's committed monthly service fee for the contracted security service for the day in which the failure occurred, not to exceed 30 days of fees.

**"Emergency Maintenance"** means any activity that Kyndryl, in its sole discretion, deems necessary to correct an immediate threat to the ongoing availability and quality of EDS Service offerings

**"Managed Kona Site Defender Response Service SLA Violation"** – the inability of the EDS support team to meet the Response time or Live Support Availability as defined.

"**Managed Kona Site Defender Service Initial Response Time"** (applicable only to Support Requests filed against the Kona Site Defender product under Managed Kona Site Defender Service) is the time it takes Customer to get a response on the reported issue from an EDS technical support representative.

The measurement of the initial response time is the elapsed time from the start of the Security Incident Management process to the response to Customer by an appropriate service resource to acknowledge the request, respond with a service request number and begin working the issue. This includes time until a response is received in the form of a call back or e-mail or any other customer facing communication. The degree of urgency can vary based upon the issue's priority level.

For Security Events identified through Managed Kona Site Defender Service Security Event monitoring, Security Incident Management begins once a Security Event has been observed and that event cannot be classified as a false positive and the issue is escalated to the customer.

For Security Events identified by the customer, the Security Incident Management process begins from the time the event is reported by the customer to Customer Care.

All Support Requests reported via e-mail will be considered as Severity 3.

**"Preconfigured Mitigation Control" –** (applicable only to Prolexic Routed Service) is a proactive measure deployed in peacetime, offering the ability to block malicious layer 3 DDoS traffic abuses that are destined to a customer's network.

"**Security Severity Levels"**

**"Severity 1"** -- Critical Impact: This class exhibits: a) loss or outage on any portion of a protected property, b) data breach (exfiltration or infiltration) confirmed in progress, or c) defacement of a protected property.

**"Severity 2"** – Major Impact: This class exhibits: a) degradation in performance on any portion of a protected property, b) suspected data breach, or c) excessive bot activity that may lead to intellectual property compromise.

**"Severity 3"** – Low Impact: This class exhibits: a) signs of a potential small-scale security incident (log event evidence of malicious traffic that does not impact the origin and may be false positive, b) is a proactive action;

"heightened attention" in response to a public threat, for instance, c) includes a possible fraud investigation without immediate evidence of data breach, or d) low-level site scraping

"**Service Outage"** (applicable only to Prolexic Routed, Prolexic Connect, and Prolexic Proxy) means that Prolexic Network did not respond to DNS or HTTP queries or the forwarding of IP traffic for more than sixty (60) consecutive seconds.

**"Service Validation"** is a process which tests Customer's environment and service performance, and is required for all Customers of Prolexic Routed (i.e., GRE or Connect Option).

**Time To Mitigate Service Level (applicable only to Prolexic Routed, Prolexic Connect, Prolexic Proxy, and Prolexic IP Protect)**

With respect to Customers subscribing to Prolexic Routed, Prolexic Connect, Prolexic Proxy, and Prolexic IP Protect, Kyndryl offers a service level ("Service Level") committing to the length of time that it will take Kyndryl to effectively deploy mitigation.

The Service Level begins at the time that a critical alert is generated by Kyndryl for Customers subscribed to the standard Always-On mitigation service or for Customers who are otherwise permitted to be running traffic through Prolexic Network when a DDoS attack is identified. The time of the critical alert will be determined by relevant ticket correspondence and/or critical alerts in the Customer Portal.

The Service Level for Customers subscribed to an On-Demand mitigation service, if not currently routed through the Prolexic Network, begins after a Customer notifies Kyndryl and properly routes traffic through Prolexic Network during a DDoS attack. The Time to Mitigate ("TTM") value for these On-Demand Customers depends upon the length of time for the Customer to properly route traffic through Prolexic Network, and the length of time it takes for routes to propagate to the Internet at large.

Kyndryl's Service Level for the following attack types is available exclusively to Prolexic Routed, Prolexic Connect Prolexic Proxy and Prolexic IP Protect Services Customer. Kyndryl commits to the following TTM, for each DDoS attack type, as categorized per following:

| **Attack Type** | **TTM - Time to Mitigate (typical)** | **TTM – Time to Mitigate - Guaranteed (Service Level)** |
|---|---|---|
| Any attack matching a Preconfigured Mitigation Control | | |
| | 0 seconds | 0 seconds |
| UDP/ICMP Floods | 1 minute or less | 5 minutes |
| SYN Floods | 1 minute or less | 5 minutes |
| TCP Flag Abuses | 1 minute or less | 5 minutes |
| GET/POST Floods | 10 minutes or less* | 20 minutes |

DNS Reflection 5 minutes or less** 10 minutes

| | | |
|---|---|---|
| DNS Attack | 5 minutes or less** | 10 minutes |

** Mitigation requiring traffic analysis* and *custom signature deployment*

*** Applies to DNS attacks targeting EDS IP addresses*

**Time To Mitigate Service Levels (applicable only to Kona Site Defender and Web Application Protector)**

With respect to Customers subscribing to Kona Site Defender and Web Application Protector, Kyndryl offers a service level ("Service Level") committing to the length of time that it will take Kyndryl to effectively mitigate an attack, meaning initial mitigations have been deployed and have been effective at mitigating the impact of the immediate attack.

Kyndryl's Service Level is available exclusively to Kona Site Defender and Web Application Protector Customers and applies only to attack traffic routed through the EDS platform. Kyndryl commits to the following TTM for each of the specified DDoS attack types:

| Attack Type | TTM - Time to Mitigate (typical) | TTM – Time to Mitigate - Guaranteed (Service Level) |
|---|---|---|
| UDP/ICMP Floods | 0 seconds | 0 seconds |
| SYN Floods | 0 seconds | 0 seconds |
| TCP Flag Abuses | 0 seconds | 0 seconds |
| DNS Reflection | 0 seconds | 0 seconds |
| DNS Attack | 0 seconds | 0 seconds |

**Time To Mitigate Service Level (applicable only to Kona DDoS Defender and Managed Kona Site Defender Service)**

With respect to Customers subscribing to Kona DDoS Defender and Managed Kona Site Defender Service, Kyndryl offers a service level ("Service Level") committing to the length of time that it will take Kyndryl to effectively deploy mitigation, meaning:

Initial mitigations have been deployed
They have been effective at mitigating the impact of the immediate attack.
The benefits of the mitigation were evident within the time window of the SLA.

The Service Level begins at the time that a critical alert is generated by Kyndryl for Customers subscribed and integrated to the standard Always-On mitigation service when a DDoS attack is identified. The time of the critical alert will be determined by relevant ticket correspondence and/or critical alerts in the Customer Portal.

Kyndryl's Service Level only for the following attack types is available exclusively to Kona DDoS Defender and Managed Kona Site Defender Service Customers. At a minimum, a Table Top Drill for Kona DDoS Defender, or a Threat Update Review and a Table Top Drill for Managed Kona Site Defender Service is required once annually and EDS Security Specialist recommendations must have been applied to the configuration. Kyndryl commits to the following TTM, for each DDoS attack type, as categorized per following:

| Attack Type | TTM - Time to Mitigate (typical) | TTM – Time to Mitigate - Guaranteed (Service Level) |
|---|---|---|
| UDP/ICMP Floods | 0 seconds | 0 seconds |
| SYN Floods | 0 seconds | 0 seconds |
| TCP Flag Abuses | 0 seconds | 0 seconds |
| GET/POST Floods | 10 minutes or less | 20 minutes |

| | | |
|---|---|---|
| DNS Reflection | 0 seconds | 0 seconds |
| DNS Attack | 0 seconds | 0 seconds |

** Mitigation requiring traffic analysis* and *custom signature deployment*

**Consistency of Mitigation Service Level (applicable only to Prolexic Routed, Prolexic Connect, Prolexic Proxy, Kona DDoS Defender and Managed Kona Site Defender Service)**

Kyndryl offers a 95% Consistency of Mitigation Service Level. Consistency of Mitigation is measured by analyzing the ratio of clean traffic to attack traffic that is forwarded to the Customer. Measurement of the Consistency of Mitigation parameter begins after the committed TTM has elapsed. Claims against the Consistency of Mitigation Service Level must be submitted with a packet capture of at least one hour in duration, identifying the total amount of attack traffic forwarded during the event envelope. The event envelope is defined as all or part of the period between the TTM Service Level period and the end of the attack. Evidence of forwarding of attack traffic in excess of 5% of the total traffic volume qualifies for a credit under this Service Level clause.

**Remedy for Time to Mitigate and Consistency of Mitigation Service Levels**

The TTM is based from the time that traffic is properly routed through Prolexic Network or EDS Network for On-Demand Customers or from the time that a critical alert is generated for services that are Always-On or already routed through Prolexic Network or EDS Network. The TTM is measured based upon the Consistency of Mitigation Service Level terms. During any given calendar month, if Kyndryl fails to meet the TTM Service Level as measured by the Consistency of Mitigation parameters set forth above, the following credits will be issued:

Single event – in the event that the TTM Service Level is exceeded – with mitigation not meeting the Consistency of Mitigation Service Level, Kyndryl will credit Customer's account for such month for the pro-rated charges as follows:

> Less than one hour: for (1) day of Monthly Service Fees due in respect of the affected Network Protection Services; For one hour or more, and less than 6 hours: two (2) days of Monthly Service Fees payable in respect of the affected DDoS Mitigation Services; and

Multiple Events or Single Event lasting more than 6 hours – in the event that the Time to Mitigate Service Level is exceeded – with mitigation not meeting the Consistency of Mitigation Service Level for a period of six (6) hours or more, or during four (4) or more events within a calendar month, Customer will be credited with seven (7) days of Monthly Service Fees payable in respect of the affected DDoS Mitigation, or Managed Kona Site Defender Services,

All Customers must have successfully completed a Table Top Drill, with any prefix(es) affected, within the previous twelve months in order to qualify for remedy credit under the Time to Mitigate and Consistency of Mitigation Service Levels.

In order to qualify for any applicable Service Level Agreements for Prolexic Routed (GRE or Connect Option), Service Validation must have been successfully completed by Customer, for any prefix(es) affected, within the previous twelve (12) months.

**Service Availability Service Level (applicable to Prolexic Connect, Prolexic Routed, Prolexic Proxy, and Prolexic IP Protect Service Outage)**

Kyndryl offers a service level ("Service Level") committing to 100% availability of the Prolexic platform. The service level begins at the time the customer has successfully completed integration and Service Validation for the protected properties, or the contract Billing Effective Date, whichever is later.

This Availability SLA does not guarantee the availability of all scrubbing centers concurrently. All Prolexic customers

are required to have resilience via 2 or more GRE tunnels per provisioned router or 2 or more VLLs per provisioned router connected to 2 or more scrubbing centers (Prolexic Routed with Connect option). Additional resilience is available to all customers, optionally.

Kyndryl will provide any credits to per the following: Provided Customer reports a Service Outage to Kyndryl promptly following the occurrence of an event of interruption in Service that Customer believes is a Service Outage, but in any event no later than five (5) days after the event took place, Customer shall be entitled to receive a service credit for Customer's benefit in accordance with the schedule below. Whether an interruption in Services constitutes a Service Outage shall be determined solely by Kyndryl in its sole good faith discretion supported by records, data and other evidence. If a Service Outage has taken place and Customer notifies Kyndryl as provided in this Section, Kyndryl shall provide a credit to Customer as follows:

If a particular Service Outage reported by Customer lasted for more than one minute but less than four (4) consecutive hours during a calendar month, Kyndryl will credit Customer for such month, the pro-rated charges for one (1) day of Monthly Service Fees of the amount of revenue Kyndryl receives from Customer with respect to the affected DDoS Mitigation Service(s); or

If a particular Service Outage reported by Customer lasted for four (4) or more consecutive hours during a calendar month, a credit equal to two (2) days of the Monthly Service Fees payable of the amount of revenue Kyndryl receives from Customer with respect to the affected DDoS Mitigation Service(s).

The above provision sets forth Customer's sole and exclusive remedy for Service Outages and any other interruptions or failures of EDS Managed DDoS Mitigation Service.

**Remedy – Attack Monitoring Services (applicable only to Application-Based and Flow-Based Monitoring Services)**

A Customer subscribing to the Application-Based Monitoring or Flow-Based Monitoring Service is entitled to remedy credit in accordance with this subsection should an Attack Monitoring Services - Failure to Notify Event occur, provided Customer reports the incident to Kyndryl promptly following the occurrence of an event that Customer believes is an Attack Monitoring Services - Failure to Notify Event, but in any event no later than five (5) calendar days after the event. Whether an incident constitutes an Attack Monitoring Services - Failure to Notify Event shall be determined by Kyndryl in its sole good faith discretion supported by records, data and other evidence.

If an Attack Monitoring Services - Failure to Notify Event occurs once or more times during a calendar month, Kyndryl will credit Customer's account for the pro-rated charges for one (1) day's Monthly Service Fees due for each incident, in respect of the affected site(s)' Services; and

**Availability and Performance Service Level (applicable only to App & API Protector, Kona Site Defender, Kona DDoS Defender, Web Application Protector, Web Application Firewall, Bot Manager, Bot Manager Premier, Account Protector and Site Shield)**

**Availability SLA:** Kyndryl offers a service level ("Service Level") committing to 100% availability of the contracted security service.

The Service Level begins at the time the customer has successfully completed integration and Service Validation for the protected properties, or the contract Billing Effective Date, whichever is later.

**Performance SLA:** Kyndryl offers a service level ("Service Level") committing that the security service will not impede origin performance in any period that the protected digital property is not under attack.

The Service Level begins at the time the customer has successfully completed integration and Service Validation for the protected properties, or the contract Billing Effective Date, whichever is later.

Activation of the Availability and Performance Service Level Agreements occurs once the Customer has successfully completed the following: Customer must enter and indicate the location of two valid test files for the same object (as described in II(c) and (d) above) into the SLA Activation Tool located in the Customer Portal. Detailed instructions are

provided with the SLA Activation Tool; in addition, assistance is available from the Customer's Account Manager and, for customers using the optional Site Shield solution, Professional Services. Customers using Remote Site Shield must ensure that their firewall configurations are updated to reflect changes made by Kyndryl to the Site Shield access control list no later than 60 days following notification by Kyndryl, via email or the Customer Portal, of such a change. Failure to timely update such firewall configurations will invalidate the performance portion of this SLA. The SLA will go into effect five (5) business days after the Customer enters valid test files into the SLA Activation Tool.

**Remedy for Availability and Performance Service Levels (applicable only to App & API Protector, Kona Site Defender, Kona DDoS Defender, Web Application Protector, Web Application Firewall, Bot Manager Standard, Bot Manager Premier, Account Protector and Site Shield)**

If the Service fails to meet the defined service levels, the Customer will receive (as its sole remedy) a credit equal to Customer's or such domain's committed monthly security service fee for the day for the protected origin(s) in which the failure occurs, not to exceed 30 days of fees.

The following methodology will be employed to measure the availability and performance of the security service:

**Agents and Polling Frequency**

From at least six (6) geographically and network-diverse locations in major metropolitan areas, Kyndryl will simultaneously poll a test file residing on the Customer's protected origin servers and on EDS network

The polling mechanism will perform two (2) simultaneous http GET operations using a test file on the customer's protected origin server (i.e., origin.customer.com).

One GET operation will be performed to retrieve the file directly from the protected origin server (i.e., http://origin.customer.com/testobject), or via an EDS Site Shield region if the customer is using the Kona Site Defender or the optional Site Shield solution.

The other GET operation will be performed to retrieve the file through the Service, by requesting the object from the protected origin server (ie, http://www.customer.com/testobject, where www.customer.com is CNAMEd to EDS and configured to pull content from origin.customer.com)

The test content must use a TTL of 2 hours or greater.

The test content will be a file of approximately 10 KB in size.

Polling will occur at approximately 6-minute intervals.

Based on the http GET operations described in II(b) above, the response times received from the two sources, (a) the protected Customer server (directly, or via a Site Shield region if applicable), and (b) the EDS network, will be compared for the purpose of measuring performance metrics and outages.

**Performance Metric**

The performance metric will be based on a daily average of performance for the Service and the Customer's protected production origin (measured directly, or via a Site Shield region if applicable), computed from data captured across all regions and hits. If on a given day the EDS daily average time exceeds the Customer's daily average time, then the Customer will receive (as its sole remedy) a credit equal to Customer's or such domain's committed monthly service fee for the protected property, for that day in which the failure occurs, not to exceed 30 days of fees.

**Managed Kona Site Defender Service Response Service Level Agreement (applicable only to Managed Kona Site Defender Service)**

Kyndryl agrees to provide a level of service to Customer's purchasing Managed Kona Site Defender Service as follows:

1. Response Time

Severity 1 ≤ 30 minutes (must be opened via phone)
Severity 2 ≤ 1 hour
Severity 3 ≤ 1 business day

2. Live Support Availability: An Kyndryl representative will be available live on the phone to respond to Severity 1 (Critical Impact) and Severity 2 (Major Impact) Service issues 24 hours a day, 7 days a week and 365 days a year. Live Support Availability for severity 3 (Low Impact) cases will be available during normal business hours, Monday through Friday, excluding local holidays, in the following geographies as follows:

North America (GMT – 05:00): 9:00 am to 9:00 pm ET
Europe (GMT): 08:00 am to 5:00 pm
Asia-India (GMT + 05:30): 9:00 am to 6:00 pm
Asia-Japan/Singapore (GMT + 08:30): 9:00 am to 6:00 pm

**Remedy for Managed Kona Site Defender Service Response SLA Violation**

In the event of a Managed Kona Site Defender Service Response SLA Violation, Customer must submit a written request for a credit (email request acceptable) to Customer's applicable Kyndryl relationship manager within seven days of the alleged SLA Violation. For acknowledged SLA Violations, Customer will receive (as its sole remedy) a credit equal to Customer's monthly Managed Kona Site Defender Service fee for the day in which the failure occurs, not to exceed 30 days of fees per month.

**Remedy Terms – General**

In order for Kyndryl to issue a credit in accordance with this SLA, Customer must have an account that is current with payments and in good standing with Kyndryl, and must be able to confirm that Customer has completed the Integration process, Provisioning, and/or Service Validation process for the applicable Service and, if applicable, all Prior Competing Mitigation Techniques, Fixes and Gear have been disabled or removed during any mitigation services.

Credits shall only apply for Services provided pursuant to the Monthly Service Fee and/or Monthly Service Overage Fee, and will not apply to any other Service. Customers with subscriptions for more than one DDoS Mitigation Service will only receive credits for affected portion of DDoS Mitigation Service(s). The aggregate credits to be provided in any calendar month shall not exceed 25% of the Monthly Service Fee in respect of the affected Service(s).