Table of Contents

AKAMAI SERVICES (OTHER THAN PROFESSIONAL SERVICES & SUPPORT) 1
NETWORK OPERATOR SOLUTIONS, AURA SUPPORT & HARDWARE 20
ANSWERX SOLUTIONS 25
SECURITY AND PERSONALIZATION SERVICES 26
DOMAIN NAME SERVICE INFRASTRUCTURE OFFERINGS 28
GLOSSARY 29

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 Akamai's 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 Akamai 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 Akamai, 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 is performed by developers with available configuration objects, parameters, and client-side APIs. Using the player does not require Akamai delivery Services.

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. Using the player does not require Akamai delivery Services.

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. Using the player does not require Akamai delivery Services.

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. Using the player does not require Akamai delivery Services.

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. Using the player does not require Akamai delivery Services.

Advanced Cache Control (Advanced Cache Optimization): Advanced Cache Control optimizes the cacheability of complex content on the Akamai 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.

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

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

- **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.

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

Akamai Identity Cloud (AIC): Akamai 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. Akamai 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 Akamai's discretion. Akamai 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 Akamai account team, and the customer assumes all risk related to the use of custom Javascript in AIC.

Akamai MFA: Akamai 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.

Akamai Security Foundation (ASF): Akamai Security Foundation is a set of capabilities and features designed to support Akamai's Application & API Protector and Abuse & Fraud Protection products . ASF includes API Discovery, Cloud Security Beta Channel (Direct or Indirect), DDoS Fee Protection, SIEM Integration, and Site Shield (1 Site Shield Map included; additional maps available for a separate fee).

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 Akamai API Gateway helps Customer easily manage, govern, and scale APIs that are crucial for enabling new customer-focused business models. API Gateway leverages Akamai's cloud delivery platform to provide distributed access, policy, and traffic controls for API traffic. Since this work occurs on Akamai's edge server network, it requires fewer round trips to origin, resulting in improved reliability and scale for APIs.

API Security: API Security solution is designed to protect all APIs regardless of where they run (on- or off-Akamai), 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 Akamai API Security professionals. Customers are allocated an initial amount of traffic analysis with higher amounts available for purchase; API Security will only analyze traffic for the purchased amount.

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 Akamai network 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
- Akamai Security Foundation (ASF)

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

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 before they 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.

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 Akamai 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 Akamai's 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 Akamai servers located in China and additional servers outside China. Without the ChinaCDN Service, all content is delivered from Akamai servers outside China.

Client Access Control Module (CAC): CAC supplies a set of IP addresses that Akamai 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: Akamai's 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 Akamai's content delivery platform into its cloud environment via Akamai application program interfaces and offer its customers delivery capabilities powered by Akamai'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 Akamai 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. Akamai 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. Akamai 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 Akamai edge platform, effectively reducing round trips and providing additional origin offload. Unlike DIY or third party solutions, Edge Redirector takes advantage of the Akamai 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. Akamai rewrites the requested URL on the Akamai 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 whitelists and blacklists to help offload unqualified traffic from the origin. The whitelists and blacklists use the inbound HTTP request criteria selected by Customer. Managing the evaluation of these requests via the Akamai 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 Akamai 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 Akamai platform, letting Customer run both internal and external tests from behind its firewall.

> **CloudTest Server Hours**: Customer can purchase compute hours from Akamai 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 Akamai's interface to its origin services. It works with both private origins and public cloud origins. Cloud Wrapper is an integrated part of the Akamai 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 Akamai's Services relate to Customer's compliance initiatives. It provides documentation that maps Akamai 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 to Akamai upon completion of its most recent PCI audit; and
  - An executive summary of recent quarterly network vulnerability scans performed on the Akamai 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 Akamai 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 Akamai 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 Akamai policies and procedures reviewed for the BITS self-assessment. BITS is part of the Bank Policy Institute.
- **HIPAA**: This module includes documentation on Akamai 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 the InfoSec team at Akamai's corporate offices in Cambridge, Massachusetts over a period of up to 5 consecutive business days, and it provides a deeper review of Akamai's policies and procedures relative to the Customer.

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 Akamai platform for each visitor. It also is designed so that the content should only be served to authorized users.

DataStream: 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 dev-ops 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, Web Application Protector, and App &API 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 Akamai's technical support organization of the DDoS Attack,
(c) Akamai'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, Akamai 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 Akamai 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 Akamai-maintained database of mobile devices matched via the Akamai 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 Device Characterization: Device Characterization provides information about the type of device used to send a request. To support Device Characterization, Akamai 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 Akamai delivery Service. 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 Akamai. Requires annual update of a signing key reference called a DS record.
>
> **Edge DNS Serve DNSSEC**: Enables transfer of signed zone to Akamai 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 IP Binding: Edge IP Binding allows Customer to configure hostnames to a limited set of IP addresses provided by Akamai.

EdgeKV: EdgeKV is a distributed key-value store that enables JavaScript developers to build data-driven EdgeWorker 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.

Edgescape (i.e. Edgescape, Edgescape Pro, Edgescape Enterprise, and Edgescape Enterprise Pro): Edgescape provides access to the Edgescape Database, which includes Akamai 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 Akamai). 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 Akamai Intelligent 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 Akamai as part of their digital infrastructure.

Enhanced Akamai Protocol: The Enhanced Akamai 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 Akamai edge server (i.e., an IP blacklist)
- A list of IP addresses that are explicitly accepted without further security analysis (i.e., an IP whitelist)
- 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 Akamai 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 Akamai 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 Akamai's global 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, Akamai's 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. It's the only load balancing solution that leverages the scale and speed of the global Akamai Intelligent Platform and can dynamically change the amount of traffic sent to a target data center.

Guardicore Security Platform is a security solution that is designed to enable Customer to apply micro-segmentation to minimize the effects of breaches, like ransomware, and provides network flow visibility and policy enforcement. The solution is offered on an on-premise or SaaS basis, either of which require execution of a license with Akamai. The solution 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 Akamai-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 Akamai NetStorage and must be delivered utilizing Akamai Services.

Ingest Acceleration: Ingest Acceleration is a feature of MSL3 and MSL4 that allows Customer to use Akamai's proprietary transport protocol to push live media streams to the Akamai platform.

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

Integrated Cloud Accelerator: Integrated Cloud Accelerator is an option of Cloud Embed that includes access to Akamai's 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 Akamai's 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 Akamai 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: Akamai's 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 Akamai DNS name servers respond to A and AAAA requests with corresponding Akamai edge servers capable of serving IPv4 and IPv6 HTTP(S) requests. IPV6 Feature, which includes access to Akamai's 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*. Akamai DNS name servers respond to both A and AAAA requests with corresponding Akamai edge servers capable of serving both IPv4 and IPv6 requests. It allows access to the Akamai 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 Akamai 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 Akamai 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 Akamai 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, Akamai 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 Akamai ticketing system.

Kona DDoS Defender Configuration Assistance: Kona DDoS Defender is configured by Akamai 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 Akamai’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, Akamai will, for any Akamai 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 Akamai 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 Akamai-SOCC. Once a Security Event has been recognized and categorized as security relevant, Akamai’s monitoring system opens a Security Incident from the log event and opens a ticket within the Akamai ticketing system. This ticket shall be analyzed by Akamai 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 Akamai 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 Akamai 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 Akamai platform. Customer can personalize manifests in a scalable way by offloading this function to the Akamai 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 WMS streaming.

Media Encryption: Media Encryption is designed to help limit stream ripping attacks. This mechanism enables Akamai to deliver encrypted content from an Akamai edge server to the player run- time. Media Encryption provides access to Akamai's 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 Akamai'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 Akamai'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 Akamai’s 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 Akamai.

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, Akamai's high-performance origin storage solution, is an optimized content storage solution for Customers leveraging Akamai delivery services. A key component of Akamai's 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 Akamai's 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 (Akamai Media Delivery Solutions): This Service includes high-quality static embedded object delivery from the Akamai 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 Akamai 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 Akamai 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.

Client-Side Protection and Compliance: Akamai's 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.

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 Akamai.
- 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 Akamai.
- 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 Akamai 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 IP Protect: Prolexic IP Protect is a symmetric service that is designed to protect individual Sites by directing traffic through Akamai's 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 Akamai-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 Akamai connection point and Customer.

Prolexic Security Solution - Facilitated Route-On (FRO): Available to On-Demand Prolexic

Routed Customers, FRO allows the Akamai SOCC to review Flow-based Monitoring alerts and, as determined necessary by the Akamai 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 Akamai Prolexic scrubbing platform without any action required by Customer. Unless otherwise specified in writing in the customer's runbook, Akamai 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 Akamai 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-Akamai, 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 Akamai.

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 Akamai servers located in Russia as well as additional servers outside Russia. Without Russia CDN Secure, HTTPS content is delivered from Akamai servers outside Russia.

Secure Internet Access Enterprise (SIA-E): SIA-E is a cloud-based protection product that helps enterprises improve defenses against targeted threats. It is designed to help identify data being exfiltrated using DNS, HTTP(s) or other protocols and to identify and block phishing, malware attacks, ransomware, and malware command and control traffic. It can also help identify the content category of the domain requested and block access to objectionable or inappropriate domains. It allows scanning of SaaS traffic to prevent Data Leakage from organizations.

Security Information and Event Management (SIEM) Integration: SIEM Integration allows Customer to capture event details generated by Akamai security products and incorporate those details into third party software (i.e. Customer's chosen SIEM solutions). Akamai supports a limited set of SIEM connectors, each of which is tested under conditions listed here: https://developer.akamai.com/tools/siem-integration/index.html. The SIEM connectors made available via the Akamai Developer Site (https://developer.akamai.com/tools/siem-integration/) are only samples, and Akamai shall not be responsible for fixing, modifying, or assisting with the implementation of the connectors. Customer should submit questions concerning use of a SIEM connector to Akamai's SIEM Connector Community Page (https://community.akamai.com/docs/DOC-7947-siem-connectors-downloads).

Security Monitor: Security Monitor provides access to dashboards and near real-time reports to monitor security-related activity via Akamai's 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 Akamai 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 Akamai 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 Akamai 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 Akamai 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 Akamai to change the points of presence that Akamai 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 Akamai 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 Akamai's 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.
- Akamai shall not be required to provide more than 50 Gbps of peak bandwidth throughput.
- Akamai 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. Akamai 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.

Unified Threat Shield: Unified Threat Shield (UTS) is a bundle of Akamai services that are purchased together in a single order form and is available to new Akamai customers. The standard UTS bundle includes defined entitlements for the following Akamai products: EAA, MFA, SIA Enterprise Advanced, Prolexic IP Protect, Edge DNS, GTM Standard, and App and API Protector. Integration and provisioning services are included for several of the services, and a monthly Services Optimization Assistance package is included – as defined in the Order Form.

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 Akamai 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 Akamai's global platform.

PROFESSIONAL SERVICES & SUPPORT

Please refer to Professional Services & Support.

NETWORK OPERATOR SOLUTIONS, AURA SUPPORT AND HARDWARE

The following terms are applicable to the license and use of Akamai's Aura Licensed CDN (Aura LCDN), Aura Licensed Multicast Solution (LMS), and the purchase and use of Akamai's Aura Managed CDN (MCDN) Services and Aura Hardware. Akamai's Aura LCDN Software, Aura LMS Software, Aura MCDN Services, and Aura Hardware are not authorized for resale, sublicense, or other distribution under Akamai's Net Alliance Partner Program.

Aura Advanced Analytics: Access to a default installation of the Aura Analytics functionality, called Basic Monitoring, is included in all Aura LCDN and LMS installations. It includes access, storage, static visualization, and export of all raw data generated by the Aura LCDN and LMS. Advanced Analytics, licensable for a fee, layers additional data analysis and visualization capabilities on top of the data gathered and stored as part of Basic Monitoring.

Aura Enhanced Support: Included for the applicable Aura LCDN and LMS licensed hereunder solely to the extent Aura Enhanced Support has been purchased pursuant to an applicable Transaction Document. Included for Aura MCDN Services. Aura Enhanced Support includes access to all of the following:

- Self-service configuration tools (where available)
- Named technical support account team
- Live support during regular business hours for S2 and/or S3 issues
- Live 24x7X365 support for S1 issues
- Multiple ways to contact Akamai's support team
  - E-mail: E-Mail address to be provided prior to product install
  - Online: Web address to be provided prior to product install
  - Phone: 1-877-4-AKATEC (1-877-425-2832) or 1-617-444-4699
- For Customers of Aura LCDN and LMS, includes Aura LCDN and LMS Software Release Updates, subject to any exclusions and limitations set forth herein or in the applicable Terms & Conditions.
- Enhanced Initial Response Times from the Akamai technical support team
  - 30 minutes beginning after Customer notifies Akamai of S1 issue by phone
  - 2 hours beginning after Customer notifies Akamai of S2 issue by phone
  - 1 business day or less for S3 issues
  - All Aura Support Requests reported via e-mail will be considered as S3

Service support calls or online support tickets initiated by an Aura Customer where the underlying issue is determined to reside in Customer's host environment (not in the Network Operator Solution or Akamai's network) are outside the scope of support. The following support-related tasks/services are excluded from the scope of Aura support requests: (i) services necessitated by: (A) improper operation, neglect or misuse of the Aura Software; (B) Customer's failure to maintain proper site or environmental conditions; (C) use of the Aura Software with any software or hardware for which it was not intended; (D) the fault of Customer or Customer's agents, employees or subcontractors; (E) any attempt at repair, maintenance or modification of the Aura Software performed by anyone other than authorized Akamai service personnel; (F) casualty, act of God or the unauthorized act of any third party; (G) failure or interruption of any electrical power,

telephone or communication service or like cause; or (H) any other cause external to the Aura Software except ordinary use as contemplated herein; (ii) any service or product not specifically set as Aura Enhanced Support Services hereunder; (iii) any services in support of Akamai's other Services or Aura Edge eXchange Hardware, (iv) Hardware, (v) any third party products, and (v) Professional Services, including on-site professional services, related to the Aura Software.

Feature Releases may be made available to paid subscribers of Aura Enhanced Support at no additional charge, but will not include any release, option, or future program that Akamai generally licenses separately from the Aura Software or for which Akamai charges an additional fee even to subscribers of Aura Enhanced Support. Maintenance Updates are made available to paid subscribers of Aura Enhanced Support at no additional charge. All Maintenance Updates provided by Akamai will be cumulative in nature, and Customer must install all Maintenance Updates provided by Akamai. Aura Enhanced Support does not include On-Site Services. The terms for Aura Enhanced Support do not apply to support services provided in support of any other Akamai Service. Customer must purchase Aura Enhanced Support sufficient to cover all licensed Aura Software. If Customer does not upgrade to the most current shipping Software Release, Akamai shall continue to provide support services for the Supported Program provided that Customer has paid for and maintained an active Transaction Document and provided further that such Aura Enhanced Support will not include Maintenance Updates for the versions of Aura Software prior to the most current shipping Software Release. To be eligible for Aura Support, hardware on which such Aura Software is deployed must be in good operating condition at revision levels specified by Akamai in accordance with Akamai's then-current bill of materials. If the cause of the problem is determined to be attributable to a third party product, or due to Customer's negligence, Customer shall be charged for such services at Akamai's then current hourly rates plus actual expenses incurred. To enable Akamai to provide Aura Enhanced Support, Customer shall (i) provide remote electronic access to (A) the Customer computer system running the Aura Software through the Internet via secure tunneling protocols and (B) all necessary operating data of the Aura Software, (ii) provide Akamai with all information and materials reasonably requested by Akamai for use in replicating, diagnosing, and correcting an error or other problem reported by Customer and (iii) install all Maintenance Updates.

If the initial term of the Aura Enhanced Support is not specified on a Transaction Document, the initial term shall be the one (1) year period commencing on the date which is thirty (30) days after the date of the initial delivery by Akamai of the applicable Aura Software under the applicable Transaction Document. Unless earlier terminated in accordance with the Terms & Conditions, upon expiration of the initial term of the initial Transaction Document for Aura Enhanced Support Services, (a) such Transaction Document shall automatically renew for successive annual periods (each such period, a renewal term) and (b) all Transaction Documents entered into subsequent to the initial Transaction Document during the initial term of such initial Transaction Document shall automatically be amended without further action by any party to renew for a renewal term that is co-terminous with the renewal term of such initial Transaction Document; provided that
(i) Customer has paid all applicable fees for Aura Enhanced Support to date; (ii) Akamai continues to offer Aura Enhanced Support for the Aura Software to its clients generally; and (iii) Customer does not terminate Aura Enhanced Support by providing Akamai with at least thirty (30) days written notice prior to the expiration of the applicable term. Upon any termination of a Transaction Document for Aura Enhanced Support, Akamai shall continue to provide Customer with individual Aura Enhanced Support for the Aura Software pursuant thereto and the Terms & Conditions, for the remainder of the period for which Customer has previously paid Aura Support fees to Akamai, unless otherwise agreed to by the parties in writing or unless Akamai has terminated the Transaction Document therefor pursuant to the Terms & Conditions.

Aura Hardware: MDS-HPE-AC-QTX media delivery servers sold by Akamai in connection with the license of Aura LCDN and LMS. Warranty support for Aura Hardware is provided by the Hardware Manufacturer or an authorized service provider thereof subject to the base limited warranty statements by Hardware Manufacturer accompanying the relevant Aura Hardware, if, where and to the extent applicable. If the Aura Hardware fails and the suggestions in product documentation do not solve the problem, Customer must

contact the Akamai technical support team before contacting the Hardware Manufacturer to properly analyze the cause of the problem. If Akamai determines that the problem is hardware-related, Akamai will so advise Customer and log a service incident with the Hardware Manufacturer, to the extent permissible under Hardware Manufacturer's warranty and technical support policies. Akamai will use commercially reasonable efforts to act as a point of contact with Hardware Manufacturer, if requested by Customer, in assisting to process any warranty or technical support claims with Hardware Manufacturer. To enable the

provision of warranty support during applicable limited warranty periods, Customer must:

- Maintain a proper and adequate environment, and use the Aura Hardware in accordance with the instructions furnished.
- Verify configurations, load most recent firmware, install software patches, run Hardware Manufacturer or other diagnostics and utilities, and implement temporary procedures or workarounds provided by Akamai or Hardware Manufacturer while permanent solutions are being worked.
- Allow Akamai and Hardware Manufacturer to modify Aura Hardware to improve operation, supportability, and reliability or to meet legal requirements.
- Allow Akamai and Hardware Manufacturer to keep resident on Customer systems or sites certain system and network diagnostics and maintenance tools to facilitate the performance of warranty support (collectively, "Hardware Manufacturer Proprietary Service Tools"). Hardware Manufacturer Proprietary Service Tools are third party products that are and shall remain the sole and exclusive property of Hardware Manufacturer. Additionally, Customer will:
    - Use the Hardware Manufacturer Proprietary Service Tools only during the applicable warranty period and only as allowed by Hardware Manufacturer;
    - Install, maintain, and support Hardware Manufacturer Proprietary Service Tools, including any required updates and patches;
    - Return Hardware Manufacturer Proprietary Service Tools or allow Hardware Manufacturer to remove Hardware Manufacturer Proprietary Service Tools upon termination of warranty support;
    - Not sell, transfer, assign, pledge, or in any way encumber or convey the Hardware Manufacturer Proprietary Service Tools.
- In some cases, Hardware Manufacturer may require additional software such as drivers and agents to be loaded on Customer systems in order to take advantage of support solutions and capabilities.
- Use Hardware Manufacturer remote support solutions where applicable. If Customer chooses not to deploy available remote support capabilities, Customer may incur additional costs due to increased warranty support resource requirements.
- Cooperate with Hardware Manufacturer and Akamai in attempting to resolve the problem via telephone.
- Make periodic back-up copies of Customer files, data, or programs stored on Customer hard drive or other storage device as a precaution against possible failures, alterations, or loss. Before returning Aura Hardware for warranty support, back up Customer files, data, and programs, and remove any confidential, proprietary, or personal information.
- Maintain a procedure to reconstruct lost or altered files, data, or programs that is not dependent on Aura Hardware.
- Provide Hardware Manufacturer or an authorized service provider of Hardware Manufacturer with access to the Aura Hardware; if applicable, adequate working space and facilities within a reasonable distance of the Aura Hardware; and access to and use of information, Customer resources, and facilities as reasonably determined necessary by Hardware Manufacturer to service the Aura Hardware.
- Notify Akamai and Hardware Manufacturer if Customer uses Aura Hardware in an environment that poses a potential health or safety hazard to Akamai and/or Hardware Manufacturer employees or subcontractors. Akamai or Hardware Manufacturer may require Customer to maintain such products under supervision of Hardware Manufacturer and may postpone warranty service by Hardware Manufacturer until Customer remedies hazards.
- Operate Aura Hardware within any maximum usage limits set forth in Hardware Manufacturer's operating manual or technical data sheets.
- Connect Aura Hardware with cables or connectors that are compatible and pre-qualified or

otherwise approved by Akamai.

- Not make any modifications to Aura Hardware.
- Implement any mandatory changes developed for Aura Hardware or third party products included therein promptly upon notice from Akamai or the applicable third party manufacturer. Mandatory changes are those reasonably designated as mandatory because they address safety, data integrity, or legal issues.
- Notify Akamai in writing of any changes to the Customer location of the Aura Hardware, including: order number, product serial numbers, complete physical address of the location of the applicable equipment, and Customer contact name at such location. Relocation of Aura Hardware may result in additional fees, and reasonable advance notice to Hardware Manufacturer may be required to begin any warranty support after relocation.
- Maintain, during the applicable limited warranty period, a list of Aura Hardware under warranty, including the location of the Aura Hardware, serial numbers, the Hardware Manufacturer's-designated system identifiers, and coverage levels.
- Designate a reasonable number of callers, as determined by Akamai and Customer, who may contact Akamai's technical support team for the initial report of a hardware problem or Hardware Manufacturer once an incident has been logged with Hardware Manufacturer by Akamai. Designated callers must be generally knowledgeable and demonstrate technical aptitude in system administration, system management, and if applicable, network administration and management and diagnostic testing. Designated callers must have a proper system identifier.
- Perform additional tasks as defined within each type of warranty service described in the applicable Hardware Manufacturer's limited warranty statements, and any other actions that Hardware Manufacturer or Akamai may reasonably request in order for Hardware Manufacturer to best perform warranty support.

Warranty repairs may be accomplished, at Hardware Manufacturer's sole discretion, remotely, by the use of a Customer Self Repair part, or by a service call at the location of the defective unit. Warranty service terms, service availability, and service response times may vary from country/region to country/region. Customer Self Repair parts are defined by Hardware Manufacturer at:

http://h18033.www1.hp.com/support/selfrepair/ww/replace_part.asp?myinc=e003a, or successor website. Replacement of CSR parts for which Customer self-repair is mandatory must be performed by Customer. For repairs, Customer will be charged additional fees for travel and labor costs. If Hardware Manufacturer determines that an on-site service call is required to repair a defect, the call will be scheduled between Customer and Hardware Manufacturer during standard office hours. If the location of the defective unit is outside Hardware Manufacturer's customary service zones, response times may be longer and may be subject to travel charges, reduced restoration or repair commitments, and reduced coverage hours. In order to receive on-site warranty support, Customer must:

- Have a representative present when Hardware Manufacturer provides warranty service at Customer's site.
- Notify Akamai and Hardware Manufacturer if products are being used in an environment that poses a potential health or safety hazard to Akamai and/or Hardware Manufacturer employees or subcontractors.
- Subject to reasonable security requirements, provide Hardware Manufacturer with sufficient, free, and safe access to and use of all facilities, information, and systems determined necessary by Hardware Manufacturer to provide timely warranty support.
- Ensure that all manufacturers' labels (such as serial numbers) are in place, accessible, and legible.
- Maintain an environment consistent with product specifications and supported configurations.

Response times set forth in the limited warranty statements are measured from when Hardware Manufacturer receives a valid support request from Akamai that is covered by warranty. Warranty support by Hardware Manufacturer does not cover claims resulting from the following: (a) improper use, site

preparation, installation, or site or environmental conditions or other non-compliance with the supporting material for the Aura Hardware; (b) modifications to Aura Hardware or improper system maintenance or calibration not performed by Hardware Manufacturer; (c) failure or functional limitations of any non-Hardware Manufacturer software or product impacting systems receiving Hardware Manufacturer warranty support; (d) malware (e.g., virus, worm, etc.) not introduced by Hardware Manufacturer; (e) abuse, negligence, accident, fire or water damage, electrical disturbances, transportation, or other causes beyond Hardware Manufacturer's control; (f) non-compliance by Customer with the Customer responsibilities set forth above or in any limited warranty statement applicable to Aura Hardware; and (g) any other exclusion from warranty coverage set forth in the applicable Hardware Manufacturer's limited warranty statement accompanying the Aura Hardware. Services performed by Hardware Manufacturer that are not covered by the warranty are chargeable at the applicable rates in the country where such service is performed.

HP Software EULA Supplied with Aura Hardware:

Third party software or firmware products supplied with Aura Hardware may be subject to separate license agreements as required by the supplier or manufacturer of such third party products. Use of any HP software supplied with the Aura Hardware is subject to the HP end-user license or program license agreement provided with such software and available at: https://www.hpe.com/us/en/software/licensing.html, or a successor website (the "HP EULA"). Customer's purchase of Aura Hardware and use of any such HP software in connection therewith constitutes acceptance of the applicable HP EULA. Customer may not exceed any use restrictions or authorizations (if any) applicable to such HP software. Akamai does not offer any hardware maintenance or hardware technical support for Aura Hardware, nor any enhancements to limited warranties (if any) provided by original Hardware Manufacturers of third party products included in Aura Hardware. If Customer requires additional warranties, hardware maintenance, or hardware support not expressly covered or incorporated herein, Customer may opt to purchase third party hardware qualified by Akamai for integration with Aura LCDN and LMS directly from the applicable third party manufacturer and/or any additional support for such hardware offered by a third party.

Aura Licensed CDN (Aura LCDN): Aura LCDN is a suite of licensed software that is sold to network operators that want to deliver their own content by operating their own CDN. Aura LCDN consists of the following components: Aura Management Center, HyperCache, and Request Router and Analytics. LCDN Encryption is an optional Feature of Aura LCDN.

Aura Licensed Multicast Solution (Aura LMS): Aura LMS is a suite of licensed software that is sold to network operators delivering their own content. Aura LMS enables multiple viewers to share the same ABR video stream, reducing access network demand. Aura LMS consists of Multicast Controller, Multicast Generator, Client Data Collector components and also includes a client SDK that is integrated into the carrier's CPE.

Aura Managed CDN (Aura MCDN): Aura MCDN is a managed CDN solution offered to Customers that are Operators. It consists of the following components: Aura Edge eXchange, Aura Edge eXchange Hardware, the Aura Operator Portal, and the Akamai customer portal.

MCDN Origin Guard: An optional feature of MCDN designed to provide ACL-based restriction of access to origins from only specified MCDN and Akamai global platform servers.

ANSWERX SOLUTIONS

AnswerX AnalytX: AnalytX is an optional DNS analytics associated with AnswerX Licensed. Customer works with Akamai to configure and provision AnalytX as a downloadable software server to collect, filter, and distribute DNS packets from AnswerX Licensed servers and any DNS traffic known to the platform. AnswerX Visualizer is an AnalytX option to visualize and query DNS data that AnalytX collects and gathers. The AnswerX Visualizer is downloadable and can co-exist with AnswerX Licensed.

AnswerX AuthX: AuthX is an authoritative DNS proxy licensed software solution built to secure authoritative DNS infrastructure and deliver workflow such as auto-generate responses to forward and reverse DNS queries, primarily (but not exclusively) for the IPv6 case where the address space is too large to statically configure. Other protections include protocol integrity enforcement and rate limiting for traffic to

the authoritative DNS. The software product resides on-net at the network operator.

AnswerX Cloud: For application service providers seeking to embed recursive DNS services into a broader solution with a cost effective total cost of ownership, AnswerX Cloud is a dynamic, data driven policy engine for recursive DNS. Unlike DIY with BIND, AnswerX Cloud is an SLA driven Internet service that not only is extensible and flexible with APIs but also optimizes content delivery with vertical integration into the Akamai content delivery network and its mapping capabilities. AnswerX add-ons designed to generate revenue and further drive service differentiation include Name Controls, Protect, and Search Guide.

AnswerX Disaster Avoidance: Disaster Avoidance is designed for recursive DNS service providers seeking to fortify a service with additional availability safeties. The availability safeties come in the form of a live backup recursive DNS service that stands ready to provide capacity in times of need or simply as the secondary DNS service. Events triggering this need might be a DDoS attack and general network outage. The backup or secondary service for each Customer might enable a generic DNS capacity or emulate primary policy enforcement. As a live backup service, Disaster Avoidance allows a network to switch to use backup capacity manually or automatically using liveness information that agents monitoring service quality produce for routing intelligence. Readiness traffic can run through the Service to ensure that the Service is operational and truly ready for service. Readiness traffic can be a proportion of live DNS or testing traffic. As a secondary service, Disaster Avoidance provisions as the secondary DNS in a network. A key benefit is to enable geo proximity for secondary DNS so that media delivery is optimal.

AnswerX Licensed: For network service providers seeking to (i) fortify recursive DNS service infrastructure against abuse such as DDoS attacks and (ii) improve resilience against network abnormalities and enable new services such as parental controls with an on-net technology solution, AnswerX Licensed is an intelligent recursive DNS solution that resides on-net close to the end user with extensibility, flexibility, scalability, and performance. Unlike DIY software and legacy platforms, AnswerX Licensed delivers service with a data- driven policy engine and optimizes content delivery with vertical integration into the Akamai content delivery network and its mapping capabilities. Add-ons include AnalytX for DNS analytics, Disaster Avoidance for additional resiliency, Name Controls for content filtering, Protect for malware and phishing protection, and Search Guide to help users find websites.

AnswerX Managed AANP: For network service providers that are participating in the Akamai Accelerated Network Program (AANP) and seeking to fortify recursive DNS infrastructure against abuse, improve resilience against network abnormalities, and enable new services, Managed AANP is a private service that is run by Akamai, single tenant, and dynamically policy and data driven with APIs. Unlike DIY with BIND and generic recursive DNS services, Managed AANP is flexible and extensible with APIs, optimizes content delivery with vertical integration into the Akamai CDN and its mapping capabilities, and includes an SLA. Add- ons include Disaster Avoidance for additional resiliency, Name Controls for content filtering, Protect for malware and phishing protection, and Search Guide to help users find websites.

AnswerX Name Controls: For network service providers trying to lower costs while improving the subscriber Internet experience, Name Controls uses network-based content filtering without downloads and for all devices on a local network. Unlike classic security agents and OpenDNS, Name Controls leverages an on- net DNS service with subscriber and device aware policies. Name Controls allows subscribers to control

which websites can be viewed by which end users within a location and automatically and dynamically mitigate malware and phishing sites. Name Controls is an add-on product for Cloud, Licensed, or Name Controls.

AnswerX Protect: For network service providers trying to lower costs while improving the subscriber Internet experience, Protect provides network-based malware and phishing protection without downloads and for all devices on a local network. Unlike classic security agents and OpenDNS, Protect leverages an on-net DNS service with subscriber and device aware policies. Protect is an AnswerX add-on available for Cloud, Licensed, and Managed.

AnswerX Search Guide: Search Guide helps users find websites when trying to directly navigate the Internet. The Service option engages subscribers with a service provider alternative search service for DNS errors (e.g. domain names that do not exist) and helps avoid typo squatter websites. A network operator makes money with Search Guide when a user clicks a link on a resulting search page. Links enable an

event for marketers and Yahoo! compensates the network operator for hosting an event that allows a user to navigate to a marketer's or trademark owner's website.

AnswerX Visualizer: Visualizer consists of recursive DNS data warehouse, ad hoc query system, RESTFul API and GUI with health dashboard.

SECURE INTERNET ACCESS: Secure Internet Access (SIA) includes the following individual software products listed below. Each of these products is deployed as on-premise software in the network operator's data centers or is hosted by Akamai.

SIA Content Compliance: SIA Content Compliance is a collection of licensed software components that together allow Customer to block internet domains across their subscriber base via DNS. Content Compliance is provided subject to the applicable license agreement located at www.akamai.com/product/licenses.

Required Product: DNSi CacheServe and Maintenance Support Content Compliance (perpetual only)

Optional Product: Content Compliance w/GIX Feed

SPS Reach: Reach is a collection of licensed software components that enables a communication service provider to communicate with its subscribers via in-browser messaging technology. Reach includes a campaign authoring and management interface for the creation, tracking, and expiration of campaigns. Reach must be integrated with the communication service provider's back end subscriber management system, which allows the communication service provider to target messages at subscribers with certain attributes.

SIA SMB Standard: SIA SMB Standard is a collection of licensed software components that enables a communication service provider to offer a network-based service – to their small and home office (SOHO) and small and mid-sized business (SMB) subscribers – that is designed to reduce the network security exposure applicable to small and medium size businesses. Secure Business also receives real-time threat feeds, which are continuously updated by the Akamai data science team to respond to evolving malware variants and agile phishing and social engineering attacks. The data science team uses specialized processing to validate threats and eliminate false positives. Using SIA SMB Standard's graphical web portal, business owners can also use Secure Business to block certain content and set filters for approved content. SIA SMB Standard's portal is accessible from any browser, and business owners can use it to establish profiles, adjust settings, and access a live dashboard and reports with graphs and data of threat activity and browsing behavior. SIA Remote is an optional add-on downloadable application designed to enable DNS privacy, security, and content filtering that works in conjunction with SIA SMB Standard. For devices onto which the SIA Remote application is downloaded, SIA Remote can facilitate the application of protections enabled in the work environment to networks outside of the workplace.

SIA SMB Standard Hosted: SIA SMB Standard Hosted is an Akamai-hosted Service that a communication service provider (CSP) may use to offer a network-based service to its SOHO and SMB subscribers designed to reduce network security exposure experienced by small and medium size businesses. SIA SMB Standard

Hosted also receives real-time threat feeds, which are continuously updated by the Akamai data science team to respond to evolving malware variants and agile phishing and social engineering attacks. The data science team uses specialized processing to validate threats and eliminate false positives. Business owners can also use SIA SMB Standard Hosted to block certain content and set filters for approved content using Secure Business Hosted's graphical web portal. The portal associated with SIA SMB Standard Hosted is accessible from any browser, and business owners can use it to set up profiles, adjust settings, and access a live dashboard and reports with graphs and data of threat activity and browsing behavior. SIA Remote is an optional add-on downloadable application designed to enable DNS privacy, security, and content filtering that works in conjunction with SIA SMB Standard Hosted. For devices onto which the SIA Remote application is downloaded, SIA Remote can facilitate the application of protections enabled in the work environment to networks outside of the workplace.

SIA SMB Advanced: SIA SMB Advanced is a purpose-built solution for small businesses offered in partnership with Plume, that offers connectivity, security protection, employee management and policy control, and workplace monitoring. The solution includes Plume's Workpass App and a backend monitoring

system providing performance details to Customer's support and engineering teams.

SIA Consumer Standard: SIA Consumer Standard is a collection of licensed software components that enables a communication service provider to offer a network-based service designed to (i) reduce exposure to Internet based threats such as phishing and malware (i.e. the Subscriber Safety option) and (ii) filter content that the subscriber deems inappropriate (i.e. the Personal Internet option). SIA Consumer Standard also receives real-time threat feeds, which are continuously updated by the Akamai data science team to respond to evolving malware variants and agile phishing and social engineering attacks. The data science team uses specialized processing to validate threats and eliminate false positives. Parents or heads-of-household can also use SIA Consumer Standard to block certain content and set filters for approved content using SIA Consumer Standard's graphical web portal. SIA Consumer Standard's portal is accessible from any browser, and subscribers can use it to set up profiles, adjust settings, and access a live dashboard and reports with graphs and data of threat activity and browsing behavior.

SIA Consumer Advanced: SIA Consumer Advanced is a smart home services framework, offered in partnership with Plume Inc, that includes WiFi connectivity, device and home cybersecurity and privacy protection, guest access and parental controls, home motion awareness, and personal well-being services. The solution includes Plume's Homepass App and a backend monitoring system providing performance details to Customer's support and engineering teams.

SIA Mobile Standard: SIA Mobile Standard is a mobile cybersecurity service including productivity & data controls for SMBs through Enterprise-level businesses. SIA Mobile Standard provides a self-serve portal and developer API access to allow business admins to configure policies, apply data controls for end users and have full visibility into their mobile traffic data, as well as allowing business admins to configure policies protecting end users against malware and ransomware, to restrict access to social media, assign Data Allowances for individual users or groups, throttle or cap users after a threshold is reached. SIA Mobile Standard requires providing SIM card information to Akamai.

Mobile Standard service comes with the below options:

- **Mobile Private Access** is designed to extend the enterprise private network to the mobile edge, allowing users to access business resources and services in a private data center, private cloud, or server with a client-less mobile connection.

- **IoT Private Access** is a self-managed connectivity service that is designed to allow an enterprise to securely connect and manage communications between devices at the edge and application services in the cloud and on-premises. IoT Private Access is designed to create a secure and managed private network that is isolated from the public internet. The built-in provisioning and automation features are designed to reduce the time to develop and deploy IoT projects at scale and with security. This service is designed to integrate into other IoT platforms such as Jasper.

SIA Essentials: SIA Essentials is a cloud-based service enabling ISPs to offer an essential security service to their SMB and/or residential subscribers without IT integration. Specifically, SIA Essentials equips ISPs and mobile network operators to deliver foundational web defenses to complement their Internet access services, including protecting against online threats including phishing, ransomware, viruses, and malware. SIA Essentials utilizes continuously updated, real-time threat feeds to respond to evolving malware variants and agile phishing and social engineering attacks.

SIA ThreatAvert: ThreatAvert is a collection of licensed software components that protects a communication service provider's (CSP) DNS infrastructure from a number of Internet-based threats such as DDoS attacks, pseudorandom subdomain and other amplification attacks, and toll fraud attacks and DNS tunneling. ThreatAvert receives real-time threat feeds, which are continuously updated by the Akamai data science team to respond to evolving malware variants and agile phishing and social engineering attacks. The data science team uses specialized processing to validate threats and eliminate false positives. ThreatAvert provides the network operator with detailed reporting covering interaction with the DNS infrastructure such as top domains queried, top clients making DNS queries, and top active threat types.

DOMAIN NAME SERVICE INFRASTRUCTURE: Domain Name Service Infrastructure (DNSi) consists of

the following individual software products (a) DNSi AuthServe, (b) DNSi Big Data Connector, and (c) DNSi CacheServe. Each of these products is deployed as on-premise software in the network operator's data centers.

DNSi AuthServe: DNSi AuthServe consists of an authoritative DNS server designed to enable resilient, secure, always-on name services. Unlike multi-purpose DNS servers, it is optimized for the authoritative function with a purpose-built database for performance and scaling. It includes management features that support complex operational environments and minimize staff overhead. Additionally, it automates lifecycle management of DNSSEC and provides real-time visibility and composite zones to simplify operations. DNSi AuthServe may be licensed on a perpetual or term basis. Support and maintenance are purchased separately and on an annual basis.

DNSi Big Data Connector (BDC): The BDC is software designed to integrate DNS and other data gathered from the following Akamai solutions with big data systems or purpose-built applications: DNSi CacheServe, SPS ThreatAvert, SPS Secure Consumer, SPS Secure Business, and SPS Reach. BDC transforms Akamai proprietary data into a JSON format so that big data systems like Hadoop, Splunk, or others can consume it. BDC may be licensed on a perpetual or term basis. Support and maintenance are purchased separately and on an annual basis.

DNSi CacheServe: DNSi CacheServe consists of a recursive DNS server that has been optimized to reduce query latency and increase Internet nameserver availability to improve responsiveness of applications and services. Customer can set fine-grained policies to manage unwanted traffic and secure and personalize home and business network access. It includes built-in security defenses against cache poisoning attacks, which can impact subscribers. It includes features that gather DNS query and server telemetry data to support operations, planning, and business initiatives, and it also provides a reporting package that includes an at-a- glance view of DNS resolution and server status and comprehensive drill-downs to details. DNSi CacheServe provides DNS extensions for better mapping between content sources and requesters, and it may be licensed on a perpetual or term basis and priced by capacity or number of subscribers (to support virtual environments). Support and maintenance are purchased separately and on an annual basis.

DNSi DCS Leases: DNSi DCS Leases are a measure of capacity enabled on the DNSi DCS server. Leases can be purchased in bundles of various sizes to fit the network in which DNSi DCS is being deployed. DNSi DCS Leases are purchased on a one-time basis. Support and maintenance are purchased separately and on an annual basis.

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 Akamai 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.

ACL: Access Control List

Active Subscriber: Any Subscriber that is actively using Customer's products and services that are enabled by Customer's use and deployment of the AnswerX Solutions, at any given time.

Akamai SOCC: The Akamai Global Security Operations Control Center Team.

Akamai University: Instructor-led Akamai training courses, either web-based or located at an Akamai training facility.

All-In Subscriber: All Subscribers that have the ability to use Customer's products and services that are enabled by Customer's use and deployment of the AnswerX Solutions, at any given time, without regard to whether all such Subscribers are actually actively using any such product or service.

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 Akamai 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.

Aura Edge eXchange Hardware: A hardware server that is deployed in an Operator's CDN to enable delivery of AEX.

Aura Operator Portal: The Aura Operator Portal is a SaaS-based management and reporting tool for Aura MCDN Customers that provides capabilities to monitor traffic delivered by the Aura Edge eXchange and Akamai Accelerated Network Program (AANP) nodes (if any).

Aura Software: Akamai's Aura branded licensed CDN software solutions offered to Customers that are Operators, including Aura LCDN and any licensed software options for use therewith.

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 Akamai Professional Services to complete a product configuration change to the Customers Akamai production configuration. Changes are limited to those possible through existing Customer interfaces for Akamai Services including the Akamai Control Center, Property Manager, Certificate Provisioning System interface.

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, Akamai 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. Akamai 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.

Cloud Partner: An Akamai reseller or Net Alliance Partner that sells Cloud Embed - Wholesale Delivery and/or Cloud Embed – Integrated Cloud Accelerator to its Subcustomers. Subcustomers will not be assigned their own individual CP Codes in the Akamai systems. A Cloud Partner will have access to usage detail reports for each of its Subcustomers, based on the identifiers it provides Akamai. Cloud Partner Product Accessibility and Serviceability Features include access for the Cloud Partner (and not the Subcustomer) to: (i) the customer

portal to set one or more configurations with appropriate included features turned on to support delivery for its Subcustomers; (ii) RESTful APIs to create individual Subcustomer profiles with Subcustomer identifier and country location and set policies for included features for Cloud Embed - Wholesale Delivery and Cloud Embed – Integrated Cloud Accelerator; (iii) RESTful APIs to access billing, usage, errors, and offload statistics at the individual Subcustomer and Delivery-Geo level; (iv) RESTful APIs to provision and manage HTTPS properties and digital certificates; and (v) Enhanced Log Delivery Service with Subcustomer identifier and Delivery Geo.
Cloud Partner must
(i) create individual Subcustomer profiles with Subcustomer identifier and country location via RESTful APIs;
(ii) configure Subcustomer policies for Cloud Embed - Wholesale Delivery and Cloud Embed – Integrated Cloud Accelerator features via RESTful APIs; and (iii) make available to Akamai Subcustomer profiles, Subcustomer identifier and Subcustomer policies.

Committed Information Rate (CIR): CIR is the maximum rate of Clean Bandwidth that Customer may pass through the Akamai scrubbing centers as detailed on the order form. The CIR should be selected such that the Customer's 95th percentile traffic should not normally exceed the contracted CIR, and such that the peak traffic does not exceed twice (2X) the contracted CIR.

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 Akamai 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 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 Akamai 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.

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 Akamai mutually agree that the traffic spike is malicious, and/or unwanted, and Customer requests Akamai to declare the traffic as a DDoS Attack, and (iii) Customer informs Akamai that they are willing to NOT serve the unexpected traffic and are willing to allow Akamai 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: Akamai's 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.

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

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 Akamai 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.

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 Akamai.

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

Network Operator Solution: Network Operator Solution means, collectively, the applicable Aura LCDN licensed by an Aura Customer and/or Aura MCDN Services purchased by an Aura Customer pursuant to a Transaction Document.

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 Akamai within 24 hours then Customer shall disengage and redirect traffic over normal routes. Any Prolexic On-Demand customer that is formally notified by Akamai

in writing that they are required to route traffic off of the Prolexic platform will be subject to being billed for their monthly 95%ile clean traffic usage at the contracted overage rate if they do not comply to the route-off request within 24 hours of notification.

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
        - In cases where a partner is providing Level 1 support to the end customer, SLAs apply to first contact with Akamai Support and the response to the Partner on behalf of the Customer.
    - Premium case status updates--Hourly for S1 issues. Less frequent updates may be provided when mutually agreed by Customer and Akamai.
- Premium Support Customer Engagement Guide
    - Communication, escalation, maintenance, and change management processes all following a custom operations support guide.

Primary Major Geography: Akamai 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. Akamai proactively monitors issues on the Akamai 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 Akamai's security Services. Proactive Service Availability Monitoring is available with Akamai's Premium Support Services.

Product Support: The provision of telephone or web-based technical assistance by Akamai to Customer's technical contacts with respect to errors related to the corresponding products and features licensed for use on the Akamai 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 and service levels included in http://www.akamai.com/service for each of these variants. Product Support does not include assistance related to errors encountered under the use of Akamai products for any purpose not stated in the service description or features of the supported products licensed by the Customer.

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

- Support for product Errors encountered by the Customer
- Initial response and acknowledgement of Security Events identified and reported to Akamai 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 Luna Control Center
- Akamai 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, Akamai 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 Akamai, monitoring of Customer bridge calls by Akamai, or the Professional Services required to identify or assess attack vectors, conduct attack response planning, provide 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 Akamai 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 Akamai 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.

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 Akamai 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 Akamai platform, reporting feeds, or invoicing. Each such digital property may consist at most one domain and ten hostnames.

Server Entitlement: The unit of measure for the number of Servers on which a Customer of Aura LCDN or Aura Object Store is entitled to run the applicable Software. One Server Entitlement is equal to one (1) Server, where a "Server" is a single physical computer comprised of processing units, memory, and input/output capabilities. Each separate physical device (e.g., a blade or a rack-mounted device) that has the required components is considered itself a separate Server.

Service Level Agreement or SLA: A service level agreement that corresponds to a particular Service

Service Validation: A process that tests Customer's environment and service performance and is required for all Customers of Prolexic Routed (GRE or Connect Option). To qualify for any applicable Service Level Agreements for Prolexic Routed (GRE or Connect Option), Service Validation must have been successfully completed by Customer within the previous 12 months.

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 (Aura support requests): The following is a guide for assigning appropriate severity levels for Aura support requests:

Severity Level	Impact	Description

Severity 1 (“S1”)	Critical	Catastrophic impact to business operations. The Network Operator Solution is significantly impaired and unavailable to multiple user locations, e.g.: ● Network Operator Solution is down causing end-users to experience a total loss of service. ● Continuous or frequent instabilities affecting traffic-handling capability on a significant portion of the network/system ● Creation or existence of a safety hazard.
Severity 2 (“S2”)	High	Significant impact to business operations. Repeatable inability to use the applicable Network Operator Solution, e.g.: ● Network or system event causing intermittent impact to end-users. ● Loss of redundancy ● Loss of routine administrative or diagnostic capability
Severity 3 (“S3”)	Low	Limited impact to business operations. Non-urgent matter or information request, e.g.: ● Issues seen in a test or pre-production environment that would normally cause adverse impact to a production network. ● Information requests ● Clarification of documentation

Severity Level (Cloud Security Services): The following is a guide for assigning appropriate severity levels for Product Support for Cloud Security Services. Akamai’s security analysts will perform an analysis of a Security Event. Whether a Security Event is considered a Security Incident is determined solely by Akamai. Identified events will be classified, prioritized, and escalated as Akamai 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 Akamai’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 Akamai edge server.

Subcustomer: A Cloud Partner’s customer for Cloud Embed.

Subscriber: A user that has a business agreement with Customer for use of such Customer’s products and services. Akamai’s records of the number of Subscribers of any type (e.g., Active or All-In) shall be determinative. Akamai will review on a quarterly basis the number of Customer’s Subscribers against the number of Subscribers of the relevant type (e.g., Active or All-In) purchased by Customer pursuant to a Transaction Document. In the event that Customer’s actual number of the applicable Subscribers during the most recently completed quarterly period exceeds the number of Subscribers purchased (such excess, the

"Subscriber Overage"), Akamai shall be entitled to invoice Customer, and Customer hereby agrees to pay additional fees at the applicable rate set forth on the Transaction Document for such Subscriber Overage for the remainder of the Term.

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 Akamai 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 Akamai Services or Akamai network) or other requests outside the scope of support. Additional Support Requests beyond those included in a particular Service package may be subject to Akamai's standard rates.

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.

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

Workload Entitlement: The unit of measure for the amount of capacity up to which a Customer of Aura LCDN is entitled to utilize the applicable Software at any instant in time. One (1) Workload Entitlement for Aura LCDN is equal to either 1 Gbps or 2000 HTTP requests per second of delivered capacity and shall be set forth on the Transaction Document.