Table of Contents

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 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 – 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 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.

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.

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.

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.

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 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 as well as aggregated metrics through PUSH & PULL APIs 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.

Enterprise Threat Protector (ETP): ETP is a cloud-based external DNS infrastructure that helps enterprises improve defenses against targeted threats. It is designed to help identify data being exfiltrated using DNS, and to identify and mitigate phishing, malware attacks, ransomware, and malware command and control traffic. It can also identify the content category of the domain requested and block access to objectionable or inappropriate domains.

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.

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 licensed or Software-as-a-Service ("SaaS") basis and is comprised of the following components and service:

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

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

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

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

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

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

Prolexic 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 Proxy: Prolexic Proxy 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 supports protection of traffic on port 80. Port forwarding is available for port

443 HTTPS traffic.

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.

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.

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.

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

Professional Services: Unless otherwise indicated, Professional Services are charged on an hourly basis at the rate set forth in the Transaction Document. If no rate is indicated, Akamai's then current list price shall apply. Depending on the nature and scope of the project, a separate statement of work may be required. Except as specified in the Transaction Documents and herein, nothing herein is intended to grant any rights, by license or otherwise, to Akamai's intellectual property or intellectual property rights. Per terms of the applicable Transaction Document, upon completion of integration, Akamai Professional Services will alert Customer to the availability of the Service. For any Professional Service engagement, Customer shall, in a timely manner, provide technical resources to answer any technical questions that Akamai personnel may have regarding requirements and deliverables. Customer will be responsible for coordinating and managing any changes to its infrastructure that may be required for integration as referenced in the applicable Transaction Document. Customer will be responsible for conducting functional testing via Akamai for all web properties referenced in the associated Transaction Document prior to going live on the platform. Only those web properties referenced in the associated Transaction Document shall be in scope for a given Professional Services engagement. Managed Integration Services are not available for web properties that require custom user client, other than standard web browsers. Unless otherwise indicated in a Transaction Document, Managed Integration Services are limited to up to 40 hours of assistance from Akamai technical professionals.

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

Included features:

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

Advanced Monthly Service Report

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

Advanced Semi-Annual Service Review

- Semi-Annual Service Report to be presented to the Customer at the end of the 6 month period.

- Semi-Annual Report Includes a Plus and Advanced Health Check review
  - Plus and Advance Health Check review is a programmatic check to match the configuration of an implementation with recommended practices.
  - Semi-Annual Report may include recommendations based on analysis of support cases and Configuration Assistance requests.
- Semi-Annual Report and Health Check covers up to the number of Health Check Configurations included on the Customer Order Form.
- Semi-Annual Service Report and associated Advanced Health Check covers up to 1000 hostnames per configuration.

Advanced Technical Advisor

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

*Note: As of November 7th, 2020, the number of Technical Advisor quarterly hours will be indicated directly in Customer's Agreement through separate contract line items indicating the included hours per quarter and overage rate. Technical Advisory Hours in excess of the total number mentioned in the Transaction Document are subject to overage charges at the hourly overage rate specified in the Transaction Document. (Note: The rate for Technical Advisory overage is different than the rate for hourly Professional Services Overage rate.)

In cases where the Technical Advisor Hours and Overage rate are not included on the Customer's applicable Transaction Document, the default will be 3 business days effort per quarter (24 hours/quarter.)

In cases where the Technical Advisor Hours and Overage rate are included on the Customers applicable transaction document, those amounts would over-ride the default.

Advanced Technical Support

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

Advanced Professional Services

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

Configuration Assistance

- Ongoing, professional services to assist with configuration of the covered Web Performance or Media Products listed on the applicable Customer Order Form.
- Up to the specified hours on the Order Form per quarter (default of 30 hours per quarter Configuration Assistance in excess of the available quarterly hours will be billable at overage rate included on the Customer Order Form.
- Upon completion of the request, Akamai will respond to the Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request.
- Advanced Configuration Assistance does not include coverage for Akamai Security products
- Work to be conducted at mutually agreed upon dates and times during Customer Business Hours.

Advanced Akamai University Virtual Classroom Training

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

Advanced Project Management Option

- Additional Paid Service Option for Advanced Service and Support that provides an aligned project coordinator
  - Gaps between the setup and recommended practices identified during the Monthly Service Report and Health Check will be triaged by the IAT and get scheduled to be updated.
  - Weekly Project Report
  - Up to 1 Weekly Project Report to be shared with the customer at the end of every week except the weeks when the customer is receiving the Semi-Annual Service Review or the Monthly Project Report.
  - Advanced Project Management is limited to the equivalent of 3 business days effort per quarter and is subject to overage at the hourly PS Overage rate on the Customer Order Form.

*Note: As of November 7th, 2020, the included amount of Project Management services will be indicated directly in Customer's Agreement through separate contract line items indicating the included hours per quarter and the applicable overage rate. Project Management Hours in excess of the total number mentioned in the Transaction Document are subject to overage charges at the hourly overage rate specified in the Transaction Document.

In cases where the Project Management Hours and Overage rate are not included on the Customer's applicable Transaction Document, the default will be 3 business days effort per quarter (24 hours/quarter.)

In cases where the Project Management Hours and Overage rate are included on the Customer's applicable Transaction Document, those amounts would over-ride the default.

Broadcast Operations Control Center (BOCC): The BOCC is a 24x7 proactive monitoring service that combines people, processes and tools to help support media Customers and minimize broadcast quality issues for specified channels. It is available for Customers who use Media Services Live as well as Premium Service & Support. For purposes of BOCC, a "channel" is a unique CP code/stream ID combination. Customer may change its selection for channel(s) to be monitored by the BOCC on a quarterly basis, unless otherwise approved by the BOCC. A minimum of 24-hours' notice is required to implement changes in Customer's channel selection.

The BOCC includes the following:

Initial Configuration Review

- The configuration review will occur when a new channel is added to the Service during the onboarding process
- The configuration review is carried out by the BOCC and the Akamai integrated account team. The review is designed to ensure that Customer's media workflows are compatible with the BOCC.
- The configuration review does not include implementation of any suggested configuration changes. Configuration changes may be facilitated through a statement of work for Professional Services - Enterprise configuration assistance.

24x7x365 Monitoring, Alerting, and Mitigation

- Monitoring of Akamai's media streaming system components for availability and quality with regularly scheduled system checks.
- Automated alerting for system component availability, content quality, and audience experience for the Customer specified, BOCC supported, workflow.
- Audience experience alerting is available only for Customer provided client–side data.

Reporting & Recommendations

- Activity report with statistics on alerts, cases and traffic volume.
- Operational Reports: Reports showing trending data, key case resolution data, and configuration and workflow recommendations, including recommended changes and other best practices. Additional professional services can be purchased to implement configuration optimization recommendations.
- After Customer receives the Activity and Operational Reports, Customer may schedule a telephone conference to discuss the reports.

24x7x365 Dedicated Hotline

- Customer will have access to a 24x7x365 BOCC hotline to directly engage the BOCC team.
- Support will be provided only for specified channels that are covered by the BOCC. Channels outside of the BOCC will receive standard Akamai Customer support.

Live Event Monitoring

- The default package will include up to one live event monitoring per month, subject to 24 hours' advance scheduling by Customer.
- The live event will include up to 1 million concurrent viewers.
- The live event will consist of monitoring of specified event channels for up to 4 hours.
- A live phone bridge will be available throughout the duration of the event.
- Pre-event checks will be performed for specified event channels.
- Monitoring reports will be delivered to Customer during the event.
- A post-event summary report will be delivered to Customer.

- Customer can order additional live event monitoring for an additional fee. A minimum of 72-hours' notice is required for configured channels. A minimum of 14 days' notice is required for non-configured channels.

Akamai Broadcast Operations Control Center Time to Respond and Time to Notify

- 15 minutes or less for Severity 1 issues (cases must be raised via phone)
- 30 minutes or less for Severity 2 issues
- 12 hours or less for Severity 3 issues

Severity Level Impact Description

- Severity 1 ("S1") Critical: Service being monitored is significantly impaired as reflected by material audience drop, rebuffering spike or start up time.
- Severity 2 ("S2") Major: Service being monitored is moderately impaired as reflected by audience drop, rebuffering spike, or start up time.
- Severity 3 ("S3") Low: Non-urgent matter or information request. Examples: Planned configuration change request, information requests, reports or usage questions, clarification of documentation, or any feature enhancement suggestions.

BOCC does not include the following, which will require a separate statement of work or change order:

- Any services or requests for configuration changes not explicitly listed above
- Any Customer requests for non-contracted channels
- Any additional live events or additional support not explicitly listed above
- Any load testing
- Monitoring of components not under the direct purview of Akamai.

CIAM Enhanced Support SLA: CIAM Enhanced Support SLA offers Akamai Identity Cloud Customers quicker issue resolution with faster response from Akamai. The Service provides the following in addition to all items included with Standard Support (as set forth on the applicable Transaction Document or in the Service description of the applicable Service):

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

CIAM Managed Integration Services: CIAM Managed Integration is intended to help Customers configure and enable the necessary services and tools to support the production deployment of CIAM solutions.

The service includes:

- Project management
- OpenID Connect enablement
- Registration/integration configuration
- Integration support
- Production release and launch support

Additional Terms:

- A Professional Services consultant will be assigned as the point of contact for the duration of the project.
- Only one implementation strategy, flow configuration, and login API client will be supported.
- The project will start no earlier than 2 weeks from the data of contract signature.

- Communication with the consultant should be submitted through the Akamai customer portal rather than by email. Consultants are available from Monday to Friday (excluding holidays), between 8:00am to 5:00pm Pacific Time, unless otherwise noted and agreed upon in the applicable Transaction Document
- Customer will provide timely access to any resources, personnel, or information necessary for the success of the project
- Services will be delivered remotely, and will not include onsite travel or support
- Additional availability regions will require a change order and/or incur additional license and deployment costs
- Requirements and integrations not covered specifically in this document may require a change order and/or incur additional license and deployment costs
- Akamai may engage subcontractors to assist in providing the Services to be delivered
- Travel requests for the Professional Services team to attend a Customer onsite visit will require an order form for the associated travel costs
- Detailed "in scope" and "out of scope" activities will be listed in the applicable statement of work or other Transaction Document.

CIAM Managed Integration Services - Additional Region: This Service option is intended to help Customer configure and enable the necessary services and tools to allow for configuration of its CIAM solution in an additional region. The Service includes:

- Project management
- Registration/integration configuration
- Integration support
- Production release and launch support

Additional Terms: All terms listed in the *CIAM Managed Integration* Service description apply.

CIAM Professional Services: CIAM Professional Services are optional add-on packages that CIAM Customers can buy to have Akamai experts assist in critical tasks such as testing, data migration, training, and advisory services.

Additional Terms

- Communication with the assigned Professional Services consultant should be submitted through the Akamai customer portal rather than by email. Consultants are available from Monday to Friday (excluding holidays), between 8:00am to 5:00pm Pacific Time, unless otherwise noted and agreed upon in the applicable Transaction Document.
- Travel requests for the Professional Services team to attend a Customer onsite visit will require an order form for the associated travel costs, with the exception of workshops.
- Detailed "in scope" and "out of scope" activities for each add-on will be listed in the applicable statement or work or other Transaction Document.

CIAM Professional Services – Additional Environment: The purpose of this engagement is to provision one additional non-production environment for Customers who require more than the three standard environments already covered in the CIAM Managed Integration Service, i.e. development, staging, and production.

Additional Terms: All terms associated with CIAM Professional Services apply. The following terms also apply:

- Akamai professional services will not copy any existing flow, schema, or profiles from an existing environment as part of this engagement

- Additional instances of this engagement can be purchased to deliver the set of environments that meet the Customer's needs
- This engagement covers the Akamai professional services effort to deliver an additional environment. Additional product costs may be incurred but are separate form this engagement.

CIAM Professional Services – Data Migration: Advanced Data Migration includes:

- Migration of up to 10 million user records in 3 phases:
- Sample migration
- Production migration
- Delta migration
- Migration of profiles linked to social login providers
- Support for self-service migrations via a sample migration script
- Support for password hashing algorithms
- Secure file transfer (sFTP)

. **Additional Terms**: All terms associated with CIAM Professional Services apply. The following terms also apply:

- Migrations will take place during regular business hours, Monday to Friday (excluding holidays), between 8:00 am and 5:00 pm PT, unless otherwise agreed upon in the corresponding Transaction Document
- Data migration throughput will not be less than 10,000 profiles imported per minute
- One cycle of delta migration file will be supported.
- Reconciliation delta migration will only contain records added or updated since the time of the production migration.
- Plural objects (arrays) will not be supported when importing data
- Customer will provide technical resources to answer any technical questions that Akamai may have regarding the requirements and deliverables in a timely manner (usually within 1 day of the request)
- In order to provide proper sign-off, the Customer technical resource should be familiarized with tools needed to use Akamai Identity Cloud, like the Akamai RESTful API set or the Console.
- Universally Unique Identifiers (UUID) will not be imported. Upon importing records, an Akamai UUID will be generated.
- Data transformations form Customer's legacy system into CIAM should be performed by Customer and reflected in the data migration files.

CIAM Professional Services – Configurable Identity Provider (Configurable IdP): Configurable IdP is an optional Service that enables Customer to connect to identity providers that are not part of the default set, and that adhere to standard identity protocols: SAML, OAuth2, and OpenId Connect. This provides the flexibility to add regional identity providers and also leverage standard identity protocols to share identities, easily enabling business to business use cases through self-service federation of identities. Akamai solution architects will integrate and test the new standards-based identity provider and attach it to Customer's Akamai social login service. Once this is complete, Customer will be able to configure the identity provider like any of the other default options and open up their applications to utilize this new login/registration option.

Additional Terms: All terms associated with CIAM Professional Services apply. The following terms also apply:

- The standards supported by the Configurable IdP Service are: SAML2, OpenID Connect, and OAuth2
- To validate the integration, Akamai requires the following information from the Customer:
    - The configuration details to access the identity provider. These are the client ID and secret. the Customer has as part of the production configuration. The client ID and

secret must be shared via a secure method
    - A test user that includes identifier and credentials to validate that identity provider integration. The test user identifier and credentials must be shared via a secure method.
- The OAuth2 standard in practice is less a firm standard and more of a framework. It is possible, though unlikely, that the specific identity provider could claim OAuth2 compliance but the actual delivery cannot be supported with our configurable integration pattern. Akamai may update this engagement to a custom statement of work if the integration to an OAuth2 provider is outside of Akamai's framework's ability to integrate
- For SAML integrations, Akamai will require the following metadata:
    - "HTTP-POST" binding URL
    - Mapping of values that would be returned in the SAML response
    - Certificate for connecting
    - For information on the metadata file, Customer must contact the identity provider service that Customer is connecting.
- The provisioning of the core Akamai Social Login functionality associated with AIC is assumed to have been completed when there exists a development and production environment. Customer will need to grant access to the solution architect to those applications.

CIAM Professional Services – Data Integration Design Workshop: Data Integration Design Workshop is designed to assist Customer with understanding data integration options and provide a blueprint for data integrations. Akamai will provide:

- A 2-day onsite workshop.
- Overview of the data integration options along with best practices for each one
- Analysis of the high-level business use cases for Customer data to align them with available data integration patterns
- Evaluation of risks and trade-offs for each integration option
- A framework that Customer's technical team can use to evaluate which data integration option is right for any given business process.

Additional Terms: All terms associated with CIAM Professional Services apply.

CIAM Professional Services – Enhanced Integration Assistance: This Service is designed for Customers that have complex use cases or which are still building CIAM strategies and need additional help understanding how CIAM integrates into larger business needs. This Service includes:

- Analysis of one use case and the delivery of a technical design document. This document is a technical blueprint for how the Customer can configure the Akamai Identity Cloud to meet its specific requirements.
- Delivery of two days of remote training to a team identified by the Customer.

Additional Terms: All terms associated with CIAM Professional Services apply. The following terms also apply:

- The Customer will provide use cases and subject matter experts to review the use cases and answer any questions Akamai professional service resources have about the use cases. If this is not provided, the delivery of this review will not be part of the deliverables for the engagement.
- Akamai professional services will not copy any existing flow, schema, or profiles from an existing environment as part of this engagement
- Additional instances of this engagement can be purchased to deliver the set of environments that meet the Customer's needs.
- This engagement covers the Akamai professional services effort to deliver an additional environment. Additional product cost may be incurred but are separate from this engagement.

CIAM Professional Services – Hours: CIAM Professional Services (PS) Hours is an optional service for CIAM Customers that provides technical account management and best practices advice to help Customers benefit from the speed of change and drive higher satisfaction. The Service includes:

- Assignment of a technical advisor from a pool of solutions architects to act as the main technical contact on Professional Services cases
- Quarterly Planning Meeting
- Weekly status call
- Quarterly hours report

Additional Terms: All terms associated with CIAM Professional Services apply. The following terms also apply:

- CIAM PS Hours engagement will be primarily managed by a single resource, but Customer may be supported by a larger team lead by the assigned technical advisor. Additional resources from the Akamai Professional Services team may complete in-scope activities as directed by the technical advisor. In the event that the technical advisor is not available for a period of time, another team member will provide backup support. Consultants are available between 8:00am-5:00pm Pacific Time, Monday through Friday (excluding holidays), unless otherwise noted
- Akamai will provide reporting for the hours used on a quarterly basis, to be delivered to the Customer by its assigned Akamai account representative
- From time to time, Customer may find that it needs some additional support hours to meet a project deadline or troubleshoot an unexpected issue. Additional overage hours are not guaranteed and will be provided based on the availability of Akamai resources
- For CIAM PS Hours purchased on a monthly usage basis (i.e. 20 hours/month, etc.), invoicing will occur on a monthly basis, for the previous month's usage. Any unused monthly hours cannot be rolled into the contract renewal or scheduled for future use. Any overages will be included in the reporting for that month and invoiced together with that month's usage
- For general buckets of hours purchased, CIAM PS Hours will be honored for a term of up to 12 months from contract signing, unless otherwise noted in a custom statement of work. Invoicing will occur on a monthly basis, for the actual hours used. Any unused hours cannot be rolled into the contract renewal or scheduled for future use. Any overages will be included as a last invoice at the end of the term or when all hours have been used up, whichever occurs first.

CIAM Professional Services – Performance Testing: An optional Service for CIAM Customers that is designed to provide support during a performance testing cycle. The Service includes:

- One cycle for performance testing
- The infrastructure needed to perform testing of an environment that replicates Akamai live production service personnel from the Akamai's teams of operations and Professional Services resources, which will be available during testing.
- All performance testing environments are validated by Akamai to ensure they meet Akamai's standards before they are provided to Customers.
- Performance testing is included as part of the Managed Integration Advanced package, or it can be purchased separately.

Additional Terms: All terms associated with CIAM Professional Services apply.

CIAM Professional Services – Premium Identity Provider (Premium IdP): Premium IdP is an optional service that enables Customer to connect to industry specific identity providers, such as medical identity providers, that require enablement by Akamai. Akamai solution architects will work with the Customer to enable the Premium IdP and also understand and configure the data mapping required.

Additional Terms: All terms associated with CIAM Professional Services apply. The following terms also apply:

- The list of premium identity providers are as follows: DocCheck, Doximity, Fimnet, M3 Medical Group, MediKey, Medy, OneKey (IQVia), PayPal, and Swiss Rx Login.

- To validate the integration, Akamai requires the following information from Customer:
    - The configuration details to access the identity provider. These are the client ID and secret that Customer received as part of its production configuration. The client ID and secret must be shared via a secure method.
    - A test user that includes identifier and credentials to validate the identity provider integration. The test user identifier and credentials must be shared via a secure method.
- Provisioning of the core Akamai Social Login service within the Identity Cloud is assumed to have been completed when there exists a development and production environment. Customer will need to grant access to the Akamai solution architect to those applications.
- This Service definition covers the configuration and enablement of a single premium identity provider. A Customer that wishes to configure more than one identity provider must purchase additional instances of this Service.

CIAM Professional Services – Priority Fee: Priority Fee is an optional fee that Customer can pay when it needs to prioritize the start of its Professional Services engagement. For a Customer that selects this option and pays this fee, projects will commence on the first business day following signature of the corresponding Transaction Document (instead of being subject to the usual 2-week waiting period).

Additional Terms: All terms associated with CIAM Professional Services apply. Additionally, Priority Fee commitments are subject to resource availability and must be reviewed and approved by Akamai Professional Services on a case by case basis.

CIAM Professional Services – SAML Integration: SAML Integration to the AIC console is an optional service that allows CIAM Customers to integrate the AIC console with Customer's identity access management solution via SAML. The Service is delivered by the Akamai Professional Services team and includes integration and testing, as well as enablement training.

Additional Terms: All terms associated with CIAM Professional Services apply. The following terms also apply:

- Customer must provide the following SAML specific metadata:
    - "HTTP-POST" binding URL
    - Mapping of values that would be returned in the SAML response
    - Certificate for connecting
    - For information on the metadata file, please contact the identity provider service you are connecting
- Customer must provide a test login that can be used for Akamai resources to validate the integration. If a set of test credentials cannot be provided, Akamai cannot guarantee the timeline on delivery of work, and a change order might be required to complete this configuration
- Customer will provide a resource who will be responsible for training additional agents on the new sign-in process
- SAML Integration for China console is not included.

CIAM Professional Services – Two Factor Authentication: Two Factor Authentication is an optional service designed to enable SMS-based two-factor authentication via APIs.

This style of SMS authentication supports the following use cases:

- Validation of code on all sign-ins
- Step-up authentication
- Password-less sign-in using sent code

- An Akamai solution architect will provide one of these two services:
    - New application configuration:
        - Customer does not have Two Factor Authentication enabled
        - Setup for a single application in a single availability region1
        - Supports any number of clients and messaging per client supports multiple languages
    - Update to an existing application:
        - Two Factor Authentication is already enabled and Customer is looking to modify an existing configuration
        - Update messaging to existing clients, or add new clients and messaging.

Additional Terms: All terms associated with CIAM Professional Services apply. The following terms also apply:

- Akamai solution architects will need the following before the engagement can start:
    - Customer to provide the application (and app ID) and clients (with client ID) to be configured as part of the Two Factor Authentication Service
    - Customer to provide the specific message with language code to send per client with any alternative language versions of the same message and their language code
- This Service is only available to Customers that have purchased either Akamai Identity Cloud Advanced or Akamai Identity Cloud with the additional Advanced Authentication provisioning option
- A Customer that purchases Akamai Identity Cloud with the Advanced Authentication provisioning option will automatically have the CIAM Professional Service Two-Factor Authentication Service added to its order.
- A Customer that purchases the Akamai Identity Cloud Advanced Service can optionally add the CIAM Professional Service Two-Factor Authentication Service to its order. Customers that do not do so will be unable to use Two- Factor Authentication until it is purchased and the Service configured by Akamai Professional Services.
- A Customer cannot purchase an update to an existing package as part of its initial purchase of Akamai Identity Cloud.
- Screen reader support enabled

CIAM Provisioning Service: CIAM Provisioning is designed to provision and deploy the necessary services and tools to allow for future configuration of CIAM solutions.

Activities include:

- Provisioning of 3 system environments (development, staging, and production)
- Console provisioning for admin and agent
- Provisioning of the Customer Insights analytics and reporting tool for up to 10 user accounts

Additional Terms:

- A professional services consultant will be assigned as the point of contact for the duration of the project.

- Communication with the consultant should be submitted through the Akamai customer portal rather than by email. Consultants are available from Monday to Friday (excluding holidays),

between 8:00am to 5:00pm Pacific Time, unless otherwise noted and agreed upon in the applicable Transaction Document

- Any configurations and customizations that took place in an evaluation environment will not be copied over into any development or production environments.
- Provisioning services will be delivered remotely, and will not include onsite travel or support.
- Additional availability regions will require a change order and/or incur additional license and deployment costs
- Requirements and integrations not covered specifically in this document may require a change order and/or incur additional license and deployment costs
- Akamai may engage subcontractors to assist in providing the Services to be delivered
- Travel requests for the Professional Services team to attend a Customer onsite visit will require an order form for the associated travel costs
- Detailed “in scope” and “out of scope” activities will be listed in the applicable statement of work or other Transaction Document

Customer Paid Travel: Customer Paid Travel is an optional package, which includes an additional fee, that Customer can order when Akamai experts' on-site assistance is required but not part of Customer's existing Services package. The fee applies when necessary and reasonable travel is conducted by Akamai personnel to Customer's premises or other location for authorized Akamai business, as designated by Customer. Customer Paid Travel can be purchased for one or more days with an incremental price fee based on the total number of days. Conducting work at Customer's premises will require and consume Customer's Professional Services hours in addition to the Customer Paid Travel charges. Additional Terms: Customer Paid Travel commitments are subject to resource availability and must be reviewed and approved by Akamai Professional Services on a case by case basis. Customer Paid Travel can be purchased only in addition to Customer's existing Service packages. Customer will be charged additional fees for Services hours according to Customer's existing Agreement.

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

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

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

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

A minimum of 21 calendar days of notice is required to ensure Event Support coverage for Customer’s event. Not all features listed in the event preparation are applicable without the 21 calendar days advance notice. This package, by default, supports events up to 4 hours. For longer events, Customer can order additional event hours for an additional fee. Minimum event hours required is 4 hours. Event hours include pre-event

and post-event activities performed by Akamai. The scope of professional service hours is limited to risk mitigation and quality enhancements of existing Akamai configurations.

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

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

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

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

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

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

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

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

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

LatAm Essentials Service and Support: Base level service package available exclusively for Akamai Customers in Latin America. Included features:

- LatAm Essentials Technical Support
- LatAm Essentials Professional

Services LatAm Essentials Technical

Support

Includes access to all items included in Standard Support plus:

- LatAm Essentials Service Level Agreement for Initial Response Time:
  - Engagement within one hour or less for Severity 1 issues (reported through Akamai technical support resources).
  - Engagement within 2 hours or less for Severity 2 issues.
  - Engagement within 1 business day or less for Severity 3 issues.
  - All Support Requests reported via e-mail will be considered as Severity 3.
  - Unlimited Support Requests for 1 Customer Team.
- LatAm Essentials Technical Support during Customer Business Hours available in English, Portuguese, and Spanish.
- Akamai shall make commercially reasonable efforts to provide LatAm Essentials Technical Support outside of Customer Business Hours in Portuguese and Spanish language, however there may be instances where LatAm Essentials Technical Support outside of Customer Business Hours will be provided in English.

LatAm Essentials Professional Services

- Ongoing, professional services to assist with configuration of the covered Web Performance, Media Delivery, or Cloud Security Services listed on the applicable Transaction Document.
- Up to the specified number of Change Requests on the order form per quarter (default of 9 Change Requests per quarter).
- Akamai will respond to all requests by the following business day. The response will include an estimate for the level of effort, and proposed schedule to fulfill the request, or alternatively, follow- up questions to clarify the scope of the request.
  - Customers exceeding the allocated number of change requests in a given quarter may be asked to defer work to the next quarter, or upgrade to a higher level of service that includes more requests.
- Upon completion of the request, Akamai will respond to Customer with a notification and request for verification that the request has been fulfilled. Failure to respond to this notification within 3 business days will be deemed by Akamai as verification and acceptance of resolution of the related request.
- Work to be conducted at mutually agreed upon dates and times during Customer Business Hours.
- Work effort to fulfill LatAm Essentials Professional Services may not to exceed 10 hours on any given request.
- Multiple Change Requests may be combined for any single request for work exceeding 10 hours.
- Changes are limited to those possible through existing Customer interfaces for Akamai Services including: Akamai Control Center, Property Manager, Certificate Provisioning System interface.
- LatAm Essentials Professional Services is available during Customer Business Hours available in English, Portuguese, and Spanish.
- Akamai shall make a commercially reasonable effort to provide LatAm Essentials Professional Services from an Akamai engineer who speaks the Customer's chosen language. At times it may be necessary for the service to be provided by an English-speaking Engineer.

LatAm Essentials Service and Support – Scope of Coverage

- LatAm Essentials Technical Support and LatAm Essentials Professional Services includes coverage for the Akamai Web Performance, Media Delivery, and Cloud Security Services listed on the Customer's applicable Transaction Document.
- LatAm Essentials Service and Support does not include support from Akamai Security Operations Control Center or Broadcast Operations Control Center.
- LatAm Essentials Service and Support Coverage excludes Akamai Prolexic and Network Operator Solution Services.

LatAm Essentials Service and Support coverage excludes new product integrations or implementations.

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

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

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

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

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

Managed Security Service (MSS) offers:

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

1. Proactive Monitoring and Alerting
    1. Proactive monitoring of designated Kona Site Defender policies.
    2. Proactive monitoring of designated Bot Manager Premier endpoints - currently restricted to 'login' endpoint type only
    3. Proactive Monitoring of designated Page Integrity configurations
    4. Proactive monitoring of designated App & API Protector with/without Advanced Security Management policies (excluding Client Reputation feature)
2. Security Event Monitoring and Attack Support
    1. Security Event Monitoring provides near real-time alerting originating from available SOCC notifications.
    2. These events are received and classified by Akamai. Priority assignment shall be based on event classification.

3. Proactive Detection & Notification
    1. Once an event has been recognized and categorized as security relevant, Akamai shall create a ticket within the Akamai ticketing system.
    2. Immediate assistance is available only via phone.
    3. Akamai requires 2 business days to cease performance of Proactive Monitoring and Alerting before final contract expiry
    4. For Security Events identified by the Customer, the Security Event Management process begins from the time the event is reported by the Customer to Akamai SOCC.
    5. For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage the security Professional Services team. Any time spent by the security Professional Services team will be charged against Security Configuration Assistance

       entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the security Professional Services team is engaged includes, but is not limited to, time-sensitive non-attack related requests, and attack-related requests where the mitigation solution is complex or involves significant effort.

Security Event Management

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

Akamai Security Operations Command Center Support Initial Response Times:

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

4. Akamai security analysts will perform an analysis of the Security Event. Whether or not a Security Event is considered an attack is determined solely by Akamai. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the severity classifications under Product Support for Akamai security Services
5. For Security Events identified by Customer, the Security Event Management process begins from the time the event is reported by Customer to Akamai SOCC.
6. Post Event Report

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

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

Attack Readiness

1. Security Health Checks
   Security health checks enable Customers to quantify their Akamai Service security posture with a grade - available only for Kona Site Defender and Page Integrity Manager.
2. Technical Security Review (TSR)

1. For additional detail, please see Paragraph 2 of “Professional Services – Security Optimization Assistance”.
2. In addition, for KSD, PIM, and AAP with/without ASM, the report provides a view of a Customer’s security posture in relation to their KSD/AAP with/without ASM policy(ies)/PIM configuration(s)

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

Advisory Services

1. Managed Security Consultant
   1. Named contact that acts as a single point of contact to manage Customer’s business priorities and communications with respect to the Akamai security Services on contract.
   2. Managed Security Consultant will allocate a maximum of 39 hours/quarter to addressing on his or her responsibilities for the Customer. Any overage will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form. This is not cumulative with any other Service that provides a Managed Security Consultant.
2. Monthly Solutions Report (MSR) and Customer Business Review (CBR) - available only for Kona Site Defender, Bot Manager Premier, Page Integrity Manager, and App & API Protector with/without Advanced Security Management
   1. Monthly Solutions Report is a summary of the security activity, overall security posture, professional services fulfillment, and project updates. MSR provides transparency into security operations up to once per month. MSRs will be delivered for fully integrated security Services within the scope of Service. Configurations and policies are not covered by the MSR until the integration is completed.
   2. Customer Business Review is an executive-level business review that includes such items as industry trends and Service roadmap insights. CBR highlights the value provided by the Service to the Customer’s business up to once per quarter.
   3. Upon request, Akamai will support a remote meeting to discuss the contents of the MSR or CBR, as applicable. Customer requested amendments to the content included in an MSR or CBR may be allowed, at Akamai’s discretion, but any time required to implement requested customizations will be recorded against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form. If no hourly rate is specified, the rate of $350 per hour will be used.
3. Akamai Attack Reporting
   Periodic summaries of attack trending and guidance, and a rollup of selected attack activities observed by Akamai.

Security Event Management - Change Management Process

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

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

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

mPulse Monthly Tuning Report

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

- The Monthly Tuning Report is prepared and presented per month to the Customer in a meeting for one domain.

mPulse Business Assessment

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

mPulse Professional Services

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

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

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

- Named Enhanced Support Plus Aqua Service Management: Includes access to all items included in Named Enhanced Support, plus Aqua ION Service Management.
- Named Enhanced Support Plus Terra Service Management: Includes access to all items included in Named Enhanced Support, plus Terra Alta Service Management.
- Named Enhanced Support delivery is evidenced by Customer having the ability to submit Support Requests.

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

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

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

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

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

Plus Monthly Service Report

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

Plus Technical Support

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

Plus Professional Services

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

Configuration Assistance

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

Plus Akamai University Virtual Classroom Training

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

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

- Premium Reactive Support
- Support Advocacy from a named technical support contact.
    - Up to the total number of hours per month indicated on the applicable Transaction Document
- Proactive Service Availability Monitoring
- Professional Services – Enterprise and Technical Advisory Service
    - Program management and ongoing professional services assistance
    - Access to a designated technical advisor for strategic initiative planning, engagement review, best practices
    - Limited to agreed-upon scope
    - Up to the total number of hours per month indicated on the applicable Transaction Document
- Unlimited Akamai University training seats (subject to availability of courses)
- Up to 2 days of custom on-site training per year
- Priority beta participation
    - (Note: Akamai's Service roadmap does not constitute a promise or obligation of delivery of any functionality. As part of its continuing program of product development, Akamai may, at its sole discretion, alter the design, specifications, and forecasted time-to-market of all of its products and Services on any roadmap.)
- Each Premium Support 2.0 Unit includes:
    - Premium Reactive Support—for an additional Customer Team
    - Support Advocacy from a named technical support contact.
        - Hours on applicable order form or other Transaction Document represent total Support Advocacy hours from all assigned advocates.
    - Reactive and Proactive Support for up to 10 additional Sites or Applications
- Service Delivery for Premium 2.0 Service and Support is evidenced by:
    - Delivery of Premium Support engagement guide to Customer
    - Customer ability to submit Support Requests.
    - Customer ability to submit requests related to the Professional Services – Enterprise Service package

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

- Premium Reactive Support with enhanced Service Level Agreement for Initial Response Time
  - Engagement within 15 minutes for Severity 1 issues (reported through AkaTec Support contact numbers)
  - Engagement within 1 hour for Severity 2 issues
  - Engagement within 1 business day for Severity 3 issues
  - Unlimited Support Requests for one Customer Team
- Included hours
  - Program management and ongoing assistance by Akamai Professional Services
  - Ongoing, professional services to assist with configuration of the covered web performance or media products listed on the applicable Transaction Document(does not include coverage for Akamai cloud security Services).
  - Number of hours: Up to the total number indicated on the applicable Transaction Document. Hours in excess of the total number mentioned in the Transaction Document are subject to overage rate included in the Transaction Document.
- Support Advocacy*
  - Named technical support contact to manage escalations and improve supportability over time
  - Number of hours - Up to the number of hours specified below depending on Premium 3.1 tier
    - Tier 1 - Up to 19 hours per month
    - Tier 2 - Up to 19 hours per month
    - Tier 3 - Up to 23 hours per month
- Technical Advisory*
  - Named technical advisor for strategic initiative planning and adoption of best practices
  - Number of hours - Up to the number of hours specified below depending on Premium 3.1 tier
    - Tier 1 - Up to 20 hours per month
    - Tier 2 - Up to 37 hours per month
    - Tier 3 - Up to 53 hours per month

  *Note: As of December 23, 2019, the number of Technical Advisory and Support Advocacy quarterly hours will be indicated directly in Customer's Agreement through separate contract line items indicating the included hours per quarter. After this date, Customer's Agreement may not include a designated tier; instead, the applicable Transaction Document will reflect the number of hours included in the previously contracted tier (1, 2, or 3). Technical Advisory Hours in excess of the total number mentioned in the Transaction Document are subject to overage at the hourly overage rate specified in the Transaction Document.
- Technical Business Assessments
  - A Professional Services led assessment that documents and presents findings for a specific area of a Customer's website(s)/application(s) and/or media asset delivery to be performed at a mutually agreed upon time.
    - Number of assessments: Up to the total number indicated on the applicable Transaction Document.
- Quarterly Business Review*
  - Up to 1 quarterly business report to be presented to Customer at the end of each calendar 3-month period.

  * Quarterly Business Reviews will consume Technical Advisory Hours.
- Premium Monthly Service Report*
  - Up to 1 Premium Monthly Service Report to be presented to Customer at the end of each month except the month when Customer receives the Quarterly Business Report.

    - Quarterly Business Report, Monthly Service Report and associated Health Check covers up to 1000 hostnames per configuration.

  * Premium Monthly Service Reports will consume Technical Advisory Hours.
- Weekly Project Report
    - Up to 1 Weekly Report to be reviewed with Customer at the end of every week except the weeks when Customer receives a Quarterly Business Report or a Premium Monthly Service Report.
- Health Checks
    - Ongoing service to ensure that implementations that have been enrolled are being constantly inspected for best practices
        - Akamai will periodically run programmatic checks to match the configuration of an implementation with established best practices.
        - Gaps identified between the setup and best practices will be triaged by the Akamai integrated account team and get scheduled to be updated.
        - If suitable, a review will be included in the Quarterly Business Review
        - The number of configurations enrolled: Up to the total number indicated on the applicable Transaction Document.
- Proactive Monitoring
    - Ongoing service to uncover potential, availability and configuration risks
        - Akamai proactively monitors issues on the Akamai network that may affect availability of Customer's web and media content.
        - Proactive Monitoring keeps Customer informed of issues
        - Does not include monitoring for website/application performance or Akamai's security Services.
        - Number of configurations enrolled: Up to the total number indicated on the applicable Transaction Document.
- Unlimited Akamai University seats (subject to availability)
- Up to 2 consecutive days of custom on-site training per year
- Off-Hour Configuration Assistance
    - This Service enables Premium 3.0 Customers to leverage Akamai experts to make configuration changes during off hours.
- Service Level Agreement of initial response from an expert within 60 minutes of opening a request outside of business hours.
- Limited to changes possible
- May be fulfilled by a non-aligned or pooled resource.
- Excludes changes to 'advanced metadata', Akamai's cloud security Services.
- Akamai may turn down any configuration change request
- Time spent by Akamai Professional Service toward this feature will be billed to Customer in one of two ways:
    - Based on usage at the rate specified on the applicable Transaction Document (hours utilized will not count toward available, contracted PS hours); or
    - Existing PS hours will be consumed at a multiplier of 1.5x (e.g. if Customer utilized 2 hours for a particular request, this would equate to 1.5 * 2.0 = 3.0 PS hours).

Professional Services – Akamai University: Akamai University provides instructor-led Akamai training courses and training delivered by Akamai's Professional Services members. Each purchased unit is equal to 1 one-time seat and can be used to attend any of the training instances listed on www.akamai.com/training.

Professional Services – Emergency Integration: An additional emergency integration fee may be applied to either a Standard or Managed Integration if all or part of the integration must be completed with less than 10 business days' notice. In order to accommodate timelines, the integration may be split into two tracks, with components requiring expedited implementation done separately from other components. Emergency

integrations are subject to resource availability, and integration scope and timing must be reviewed and approved by Akamai Professional Services on a case by case basis.

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

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

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

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

Professional Services – Managed Kona Site Defender Service

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

The base unit of Managed KSD Service includes:

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

An incremental monthly service fee is charged for each additional:

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

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

- Monitoring and Attack Support for additional Protection Policies

Managed KSD Service – Technical Security Review:

Technical Security Review includes analysis of security activities associated with 1 Protection Policy and its protected sites and/or applications as well as recommendations for security posture

improvements derived from that analysis. Recommendations can be implemented as updates tothe corresponding security configuration using Security Configuration Assistance hours.

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

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

Managed KSD Service – Security Event Monitoring Includes

- Security Event Monitoring provides near real-time alerting originating from available KSD notifications.
- These events shall be received and classified by Akamai. Event classification shall result in the assignment of a priority to each individual log event. Events classified with priority 1, 2, or 3 are considered security relevant events requiring further analysis and/or escalation to a Customer authorized contact.
- Once an event has been recognized and categorized as security relevant, Akamai's monitoring system shall open a ticket within the Akamai ticketing system corresponding to the Security Incident. This ticket shall be analyzed by Akamai security response staff, and escalated to the Customer's authorized contact if it is not possible to classify the incident as a false positive.

Managed KSD -- Security Event Management Includes:

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

Security Event Management -- Change Management Process

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

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

1. Technical Security Reviews (TSR):
   1.1. For additional detail, please see Paragraph 2 of “Professional Services – Security Optimization Assistance”.

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

3. Security Event Management:
   3.1. 24x7 reactive support for Security Events related to the Akamai security Services on contract
   3.2. Customers are entitled up to 40 reactive attack support cases per year across Akamai security Services by default or as defined in the Customer's Agreement with the option to purchase additional entitlements as needed.
   3.3. Akamai Security Operations Support Initial Response Times:
      3.3.1. 30 minutes or less for Severity 1 issues (must be opened via phone)
      3.3.2. 1 hour or less for Severity 2 issues
      3.3.3. 1 Business Day for Severity 3 issues
      3.3.4. All Support Requests reported via email will be considered as Severity 3
      3.3.5. Security Operations Support Initial Response Times apply only to Support Requests filed against a currently contracted security Service.
   3.4. Akamai security analysts will perform an analysis of the Security Event. Whether or not a Security Event is considered an attack is determined solely by Akamai. Identified attacks will be classified, prioritized, and escalated as Akamai deems appropriate in accordance with the severity classifications under Product Support for Akamai security Services
   3.5. For Security Events identified by Customer, the Security Event Management process begins from the time the event is reported by Customer to Akamai SOCC.

Advisory Services

4. Managed Security Consultant
   4.1. Named contact that acts as a single point of contact to manage Customer’s business priorities and communications with respect to the Akamai security Services on contract.
   4.2. Managed Security Consultant will allocate a maximum of 20 hours/quarter to addressing on his or her responsibilities for the Customer. Any overage will be charged against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form. This is not cumulative with any other Service that provides a Managed Security Consultant.

5. Additional Terms
   5.1. Readiness and Response Service does not include assistance related to the use of Akamai security Services for any purpose not stated in the service description of the contracted Service(s) consumed by the Customer.
   5.2. Security Event Management is limited to the capabilities of the supported Service.
   5.3. Security Event Management for Bot Manager does not provide defense against direct to origin attacks.
   5.4. For Security Events identified by Akamai or by the Customer, there are instances where SOCC will engage the Security Professional Services team. Any time spent by the Security Professional Services team will be charged against Security Configuration

Assistance entitlements at the hourly rate specified in the applicable Order Form (if no hourly rate is specified, the rate of $350 per hour will be used). The scope of work for which the Security Professional Services team is engaged includes, but is not limited to, time-sensitive non-attack related requests, and attack-related requests where the mitigation solution is complex or involves significant effort.

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

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

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

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

1. Named Akamai Security Expert:
   - 1.1. A designated Akamai security expert aligned with the Customer's team
   - 1.2. This expert coordinates Customer's Security Optimization Assistance deliverables, works closely with Customer's team to understand Customer's security profile and business priorities, provides contextual recommendations and also coordinates the implementation of changes to Customer's security configurations when required

2. Technical Security Reviews (TSR):
   - 2.1. Technical Security Review is an on-demand deliverable based on entitlements. The objective of the report is to present an analysis and to provide actionable recommendations.
   - 2.2. One Technical Security Review will include the review of only one of the covered security Services and the detailed scope per Service is defined in 2.9. - 2.17.
   - 2.3. A Technical Security Review for enterprise security Services (Enterprise Threat Protector/Enterprise Application Access/Enterprise Defender) requires the enterprise security coverage line item. The maximum number delivered per year is defined on the enterprise security coverage line item in the applicable Order Form.
   - 2.4. Technical Security Reviews do not include implementation of specific configuration recommendations. Those may be implemented using Security Configuration Assistance hours, or may be implemented by Customer.
   - 2.5. Upon request, Akamai will support a remote meeting to discuss the contents of the TSR. Customer requested amendments to the content included in a TSR may be allowed, at Akamai's discretion, but any time required to implement requested customizations will be recorded against Security Configuration Assistance entitlements at the hourly rate specified in the applicable Order Form. If no hourly rate is specified, the rate of $350 per hour will be used.
   - 2.6. Customers are entitled to receive up to the number of Technical Security Reviews per year as included on the applicable Order Form
   - 2.7. Akamai reserves the right to execute no more than 1/3 of the Technical Security Reviews in any single calendar quarter.
   - 2.8. Technical Security Reviews not consumed during the contract year will expire
   - 2.9. A Technical Security Review for Kona Site Defender includes:

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

2.10. A Technical Security Review for Prolexic Routed (or Prolexic Routed with Connect option) includes:

2.10.1. Analysis of one location/data center

2.10.2. Recommendations to mitigate identified issues – e.g. latency that might indicate the Customer needs to migrate to another scrubbing center for mitigation to reduce the impact.

2.11. A Technical Security Review for Bot Manager Premier includes:

2.11.1. Analysis of bot activity on up to 5 resource purpose names or endpoints with corresponding actionable recommendations.

2.12. A Technical Security Review for Web Application Firewall includes:

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

2.13. A Technical Security Review for Page Integrity includes:

2.13.1. Review for up to 1 Page Integrity configuration

2.14. A Technical Security Review for Enterprise Threat Protector includes:

2.14.1. Review of up to 1 ETP Configuration

2.15. A Technical Security Review for Enterprise Application Access includes:

2.15.1. Review of up to 1 EAA Configuration

2.16. A Technical Security Review for Enterprise Defender includes:

2.16.1. Review of one of the following: Up to 1 EAA Configuration, up to 1 ETP Configuration, or up to 1 KSD Policy covered by the Enterprise Defender package

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

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

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

3. Security Configuration Assistance:

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

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

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

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

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

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

3.7. Akamai will respond to all requests by the following business day providing either (i)

an estimated time to fulfill the request and an estimate of the number of hours to fulfill the request, or (ii) follow-up questions to clarify the request

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

4. Additional Terms:
   4.1. Security Optimization Assistance does not include assistance related to the use of Akamai security Services for any purpose not stated in the service description of the supported Services purchased by Customer
   4.2. Technical Security Reviews do not include implementation of specific configuration recommendations. Those may be implemented using Security Configuration Assistance hours, or may be implemented by Customer.
   4.3. Security Configuration Assistance is not intended to provide Attack Support

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

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

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

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

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

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

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

- Premium 3.0 Service and Support – (Premium)

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

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

The following Protect and Perform bundles are currently offered:

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

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

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

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

Self-Service Integration: A Customer that opts for Self-Service Integration must self-integrate all Services on the applicable Transaction Document without the use of Akamai Professional Services. Akamai technical support will be available at the level purchased by Customer, but Akamai technical support does not provide integration services. Akamai shall not be responsible for errors in Customer's configuration or integration if Customer has chosen Self-Service Integration.

Standard Support: Standard Support is Akamai's base level technical support. Standard Support includes access to all of the following:

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

the applicable Transaction Document or in the Service description of the applicable Service.

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

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

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 Essentials: SIA Mobile Essentials is designed to provide DNS-level customer security across SIM-enabled devices for businesses. SIA Mobile Essentials provides a self-serve portal and developer API access to allow business admins to configure policies 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 or to restrict access to social media.

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.

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 Mobile Advanced: SIA Mobile Advanced is a Network based Mobile Threat Defense product designed to

provide visibility, security, control across SIM-enabled devices along with the advanced layer 7 and SWG capabilities. SIA Mobile Advanced provides a self-serve portal and developer API access to allow business admins to configure policies, apply data controls, application control, URL filtering or blocking 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 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.
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 Configuration Assistance, or custom rule development.

Professional Services: Professional Services, including integration services, is the term used to generally encompass the Services described under the Professional Service-related entries of the 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.