A10 Lightning Application Delivery Service

Application Traffic Management, Security and Analytics in Public, Private & Hybrid Clouds

Overview

The A10 Lightning Application Delivery Service (ADS) is a cloud-native solution to optimize the delivery and security of applications and services running over public or private clouds. ADS is purpose-built for containers and microservices-based application architectures and elegantly integrates with DevOps processes.

Supported Platforms

The A10 Lightning Application Delivery Service (ADS) optimizes the delivery and security of cloud-native applications and services running over public or private clouds. For organizations embracing the cloud and application centricity, ADS increases operational efficiency, offloads IT administrators from cumbersome tasks and reduces risk.

The solution provides innovative Layer 4-7 capabilities, including traffic management with content-switching with advanced elastic load-balancing, security and analytics for applications on public, private and hybrid clouds.

- **Scale capacity to meet performance demands.** Increase application availability and operational efficiency with advanced elastic load-balancing and application security that auto-scales with demand.
- **Make smarter decisions with unique application data.** Use per-application analytics to proactively identify issues, streamline troubleshooting and effectively meet capacity requirements to deliver superior user experiences.
- **Increase agility with multi-cloud initiatives.** Achieve deployment flexibility with the ability to seamlessly manage and maintain workloads residing in private, public or hybrid cloud environments.
- **Enhance DevOps processes**. ADS is purpose-built for cloud-native applications designed with containers and microservices-based application architectures and elegantly integrates with DevOps processes.
- **Defeat cyberattacks and meet compliance requirements.** Ensure business continuity by defending against advanced and emerging attacks and ensure uninterrupted operations.

IT infrastructure administrators are able to empower application teams with a self-service model that enhances agility while providing per-application visibility and insights. Its multi-cloud capability and either an aggregate consumption-based subscription pricing model or as a self-managed platform with subscription licensing options increases deployment flexibility and lowers cost.

Architecture and Key Components

A10 Lightning ADS is purpose-built to serve not just traditional Web applications but also new-age microservices and container-based applications. The solution delivers optimized application performance, security and per-application visibility for cloud native applications.

The solution offers a highly scalable, software-defined distributed architecture with a separation of control and data planes. This allows the A10 Lightning ADC data plane elements to be lightweight and deployed close to, or embedded within, the application environment. Organizations gain centralized control of both the data plane elements and policy management from the centralized controller.

This design provides built-in high-availability and elasticity. The A10 Lightning ADCs are automatically deployed in a cluster with a scale-out architecture that is managed by the controller. With centralized management, all policies may be configured in a central place, irrespective of where the A10 Lightning ADCs are deployed (e.g., different cloud, regions, environments).

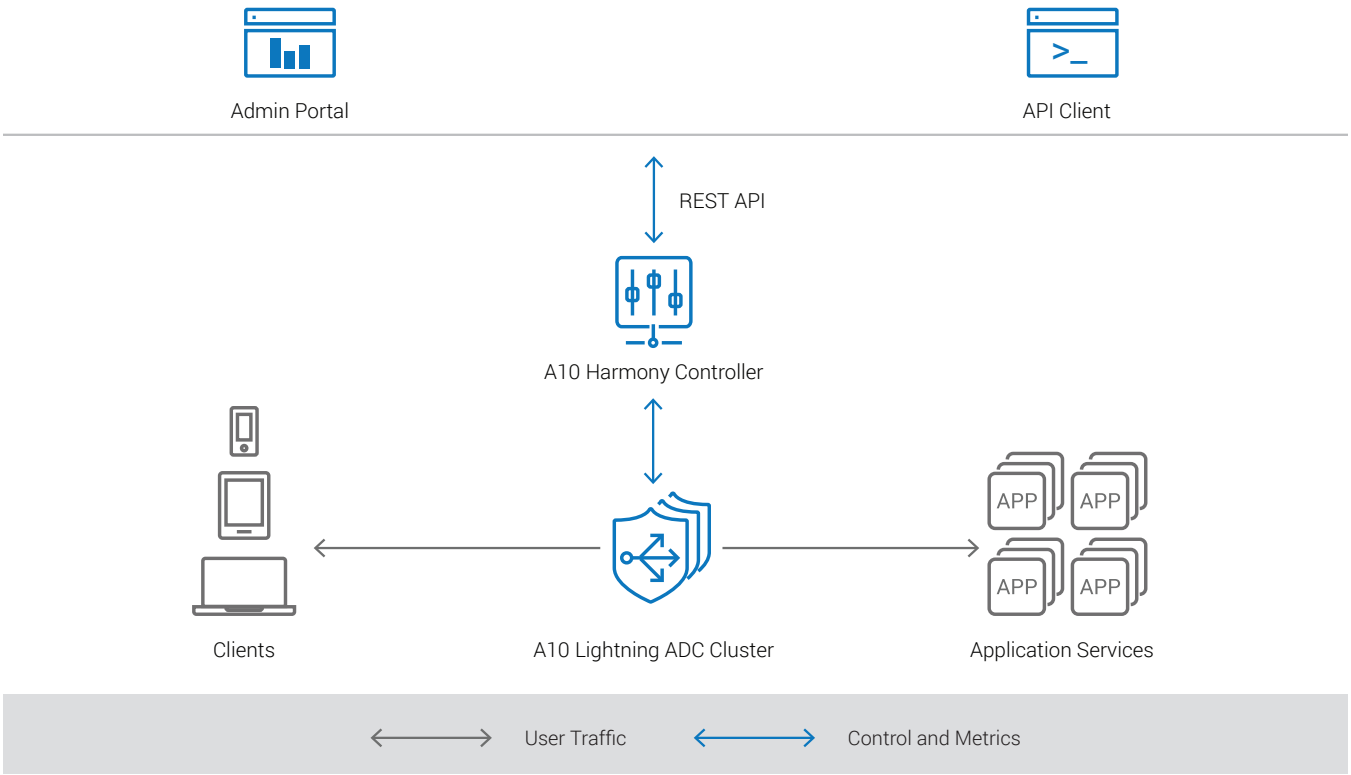


Fig.1 The A10 Harmony Controller manages A10 Lightning ADC clusters, client APIs and administrative capabilities. This deployment model helps organizations configure all policies in a central location, regardless of where A10 Lightning ADCs are deployed.

A10 Lightning ADS Components

Harmony Controller provides centralized management, policy configuration, monitoring, control and a big data repository and analytics engine. The controller manages and orchestrates clusters of software-based A10 Lightning ADC instances that implement and enforce policies.

The controller is a multi-tenant system that provides role-based access to application admins for self-provisioning of application services. It's a scalable, microservices-based application that is delivered as a SaaS by A10 or can be deployed within an organization's private cloud. With the controller, dynamically add new on-demand A10 Lightning ADCs based on load to eliminate over-provisioning.

Lightning ADC is a compact, efficient full proxy that front-ends cloud applications and microservices to execute Layer 4-7 application delivery policies. A10 Lightning ADCs are typically deployed in the network — where the application servers are running — and communicate with the controller over a secure SSL encrypted messaging infrastructure.

A10 Lightning ADC instances are stateless and are managed by the controller. Based on the traffic analytics and policies set by the admin, the controller can auto-scale the A10 Lightning ADCs to serve the application traffic.

Harmony Portal is an easy-to-use, role-based portal for managing application delivery infrastructure and associated policies on a per-application basis. The self-service capability eliminates the need for centralized IT admins to set up and configure the per-application infrastructure, maximizing agility and operational savings to support multiple application teams.

Harmony APIs make all ADS capabilities available via the RESTful interface. Orchestration and configuration APIs may be used to integrate with deployment automation tools like Chef, Puppet and Ansible, as well as continuous integration/continuous deployment (CI/CD) tools like Jenkins.

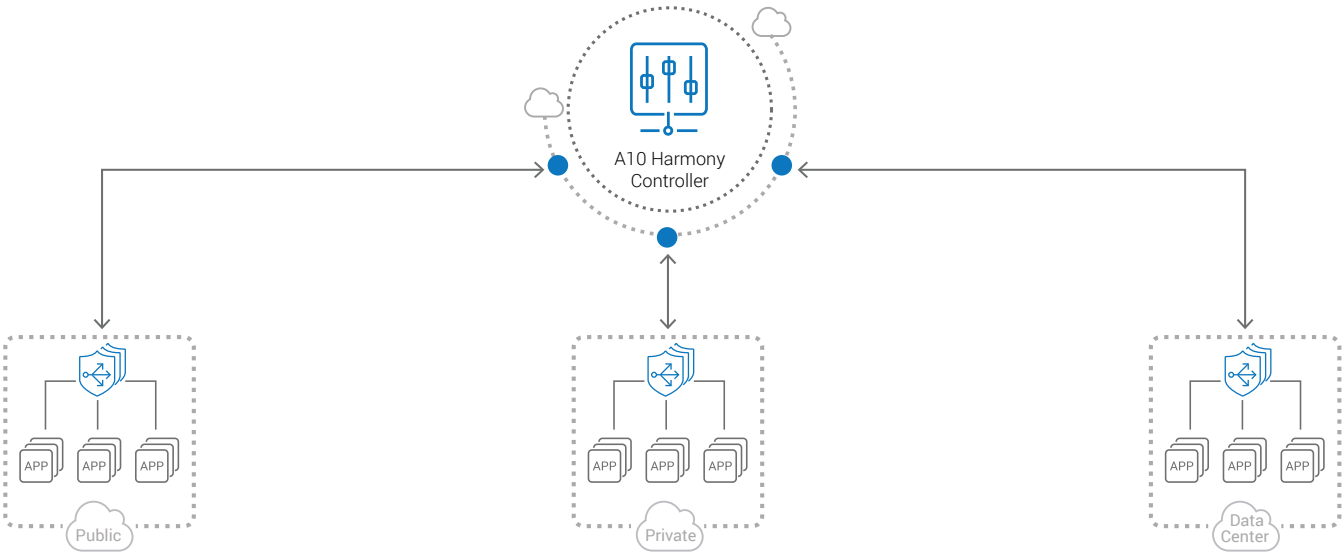
Analytics APIs also provide access to per-application metrics and logs. They may be used to integrate with third-party tools or to help build custom dashboards.

Deployment Options: SaaS and Self Managed

There are two ways to utilize Lightning ADS: SaaS or self managed. In the first option, the A10 Harmony Controller is provided as a software-as-a-service (SaaS), hosted and managed by A10 Networks. Organizations may obtain an account for the controller and start utilizing cloud-native application load-balancing, security and analytics capabilities in just a few minutes.

The self-managed option is offered as a complete platform under the full control of the organization. The Lightning ADS components are provided as a software bundle. This version operates in a similar manner to the SaaS option except the organization deploys and manages the controller in VMs within their on-premise or private cloud. The controller inter-operates with various private cloud orchestration tools.

The controller manages A10 Lightning ADCs that run inside a customer infrastructure in public clouds, private clouds or data centers. The controller is capable of simultaneously supporting instance deployments in multiple clouds for expanded scalability, flexibility and choice.



With the ADS deployment architecture, application traffic flows only via A10 Lightning ADCs (and never through the controller). With this approach, the application traffic remains secure in customer networks. Only control messages, metrics and telemetry data are sent between the controller and A10 Lightning ADCs via a secure SSL-encrypted channel.

This architecture provides two overarching deployment advantages:

- Users gain self-provisioning, agility and complete control over application traffic while customizing the configured policies to the specific application.
- Organizations significantly reduce the cost of infrastructure, as well as management overhead, that directly reduces the total cost of ownership (TCO).

Features and Benefits

The A10 Lightning ADS product line of cloud-native secure application delivery services enable customer applications to be highly available, accelerated and secure. The software-defined architecture features a light-footprint ADC that provides advanced load-balancing, Layer 7 Web security, visibility and analytics of the application traffic.

An advanced multi-tenant controller provides centralized policy management for a dynamic pool of A10 Lightning ADCs, including self-provisioning and auto-scaling, real-time per-application analytics and instantiates the Lightning ADCs to deliver an elastic, cloud-native solution. The controller is available either as a SaaS from the A10 cloud or as a self-managed solution. A10 Lightning ADCs may be deployed in public clouds, private clouds or within on-premise data centers.

Traffic Management

Leverage advanced load-balancing and server-monitoring capabilities to ensure application availability for customer satisfaction. Seamlessly scale Web and key infrastructure to meet customer demand and ensure business continuity to maximize revenue and exceed service-level agreements.

- **Layer 4-7 advanced load-balancing with auto-scaling.** Extend traditional load-balancing with content-switching and session persistence. Advanced server health checks ensure requests are only forwarded to active servers that are able to respond.
- **DevOps agility.** Leverage APIs that integrate with existing DevOps tool chains and processes, such as blue-green and A/B deployments. IT can generate 'before-after' analytics to increase the efficiency of continuous delivery.
- **Policy-based traffic management** with content-switching allows optimal management of applied policies for how user requests are fulfilled.
- **Traffic surge protection.** Temporarily queue incoming requests on the A10 Lightning ADC during traffic bursts to smooth demands on the server for improved application availability. For longer-term events, elastically scale A10 Lightning ADCs to handle sustained high-traffic levels.

Application Acceleration

Provide fast and responsive service to your end-users for a competitive advantage. Reduce infrastructure requirements for both application delivery and critical services, driving down CAPEX and OPEX.

- **HTTP/2**: Support new revisions of the HTTP protocol and decrease latency to improve page load speed.
- **Compression.** Condense requested server content to significantly reduce the transmission of superfluous content for faster response times and quicker page downloads.
- **In-memory caching.** Cache content directly on the A10 Lightning ADCs to respond faster to previously retrieved application material. Prevent added delays and remove extra loads from the servers.
- **Offload-processing for intensive workloads.** Move CPU, memory and encryption tasks to the A10 Lightning ADCs for better user experiences. Tasks such as SSL, TCP connection pooling, and rewriting of request/responses for headers and body are best handled by the A10 Lightning ADC.

Application Security

Protect against advanced and emerging attacks for uninterrupted operations, brand protection and revenue loss — all while meeting regulatory compliance obligations.

- **Elastic Web application firewall (WAF).** Use advanced rule sets to protect against top OWASP vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), plus gain application-specific security rules for popular applications like WordPress, Joomla, Microsoft Outlook Web Access (OWA), etc.
- **Defend against attacks.** Deploy advanced security to protect against malware, malicious botnets and application-layer DDoS attacks. Monitors traffic parameters to identify and protect your business from application-layer DDoS, botnet attacks and malware. Safe user traffic is permitted while the system identifies and blocks malicious traffic before it can impact app server resources and availability.
- **Access control.** Using any information available in the HTTP request (e.g., IP subnet, country, browser or any custom parameter), access control can be exercised and the user can be either blocked or can be asked to prove the identity.

Application Analytics

Ensure your organization has complete visibility and control. Provide data-driven insights and actions improve cloud application performance and health.

- **Per-application analytics.** Use insights and analytics at the application level to help application owners proactively identify issues, troubleshoot faster and quickly build capacity plans.
- **Comprehensive reporting, visualization and analysis.** Gain deeper insights into a specific metric, time range or correlation. The application dashboard gives access to a broad range metrics for application traffic, security, performance and health.
- **Centralized access logs.** Get to the root of any issue — and begin remediation efforts — with application access logs that empower application owners to easily get to the root of any issue.
- **Alerts.** Program the system to raise alerts in various conditions or a combination of conditions. Alerts are delivered via email for manual action and/or to a webhook URL for automation.

Packages and Price

A10 Lightning ADS is available in two service packages: basic and pro. Pricing is not based on the number of A10 Lightning ADC instances being used, but rather on an aggregate consumption metric. When procured as SaaS from A10, the Harmony Controller is included in both packages.

BASIC

The basic package includes traffic management, basic security and analytics capabilities.

PRO

The pro package includes all components of basic and adds the Web application firewall (WAF).

When procured as a self-managed option, the A10 Harmony Controller software license is purchased separately from Lightning ADS. It is priced on an annual subscription basis and supports both basic and pro ADS packages.

Detailed Feature List

Traffic Management

Feature	Details	Benefits
Supported Protocols	HTTP, HTTPS, HTTP/2, TCP, UDP, Websocket	Multiple types of front-end applications
Application Load-Balancing	Methods: Least Connections, Round Robin, Weighted Round Robin, IP Hash and IP-Port Hash	Deploy application instances of different sizes according to cost dynamics
Session Persistence	Persistence by: Header, Query Parameter and cookie-based session persistence	Support applications using server-side sessions
L7 Traffic-Switching	Steer traffic flows to separate pools of app servers based on any HTTP header context	Insert appropriate business logic to customize traffic flows
Granular Policy Application	Segment traffic to apply policies	Fine-grained control over the policy engine
Traffic Manipulation	Rewrite request and response headers, URLs and response body	Gain better control over data flow and flexibility to alter infrastructure as well as individual page
Traffic Optimization	Offload compression, caching	Improve utilization of server resources
Connection Pooling	Pool connections to back-end servers	Conserve server resources and improve performance
Support for Multiple Domains	Support multi-DNS domains for a single application	Quickly integrate different app domains during acquisitions or portfolio consolidation
Shared Session Information	HTTP sessions stateful information shared across all Lightning ADCs in a cluster	Delivery better client experiences
SSL Offload	Terminate SSL session on proxy and re-encrypt for end-to-end SSL	Conserve application server processor cycles
Server Health Monitoring and Use of Backup Server Group	Monitor the health of app servers and, if needed, serve the traffic using backup server pool	Improve availability of application
Built-In High Availability and Elastic Scaling of Lightning ADC	Active-Active deployment of Lightning ADC that automatically scales with traffic	Improve app availability without too much upfront investment
Blue/Green Deployments	Granular control for mirroring or steering production traffic to new deployment or pre-production application servers; app analytics between blue/green	Increase confidence and efficiency of upgrades

Security

Feature	Details	Benefits
Elastic Web Application Firewall (WAF)	Protection against top-10 vulnerabilities highlighted by OWASP	Avoid application-layer attacks and data theft
Application-Specific WAF	Pre-built application security rule sets for popular applications (e.g., WordPress, Joomla, etc.)	Easily configure and deploy for popular applications
Application Layer DDoS Attack Protection	Mitigate DDoS attack by applying tight controls	Improve service availability
Prevent Server Fingerprinting	Prevent attackers from getting access to the app server information	Reduce the chances of attack
Protection Against Malware and Known Botnets	Leverage wisdom of crowd for getting protected	Improve resource optimization and reduce infection
Access Control	Allow/deny traffic based on combinations of parameters present in HTTP request, including IP address	Improve experience for legitimate users
Session Tracking and Rate Limiting	Track sessions based on cookies or client IP and rate limit the sessions and requests within a session	Gain insights about end-user behavior and mitigate volumetric DDoS attacks
Information Protection	Block or mask the transfer of sensitive information from server to client; encrypt the data stored in cookies on the client side	Complete safety of sensitive information

Analytics

Feature	Details	Benefits
Response Time Monitoring and Details	Monitor time taken in each portion of request-response cycle	Quickly reach root of a problem and fix
Granular Insights and Analytics	Get insights and behavioral analysis at application level up to URL level	Gain better understanding of traffic and service utilization
Security Insights and Analytics	Clear display of state of security and attacks	Improve incident response times
Infrastructure Health Monitoring	Monitor server health	Take preventive action for improved application availability
Per-Request Analysis and Application Access Logs	View and analyze access logs of the application in a single place	Reach to root of the problem, differentiate one-off case from system degrade and fix quickly

Operations

Feature	Details	Benefits
RESTful APIs	Single-point integration can be achieved with DevOps toolchain	Fully automate infrastructure tasks
Multi-Tenant SaaS or Self-Managed Controller	Multiple accounts (for individual app teams) may be created	Support self-service while separating resource access
Alerts	Alerts delivered via email for manual actions; delivered via web-hook for automating the alert response	Implement a better alert response system for improved application availability

Visibility and Analytics

A10 Lightning ADS provides comprehensive visibility and analytics. Users may generate a variety of reports. The following table provide examples of the types of reports administrators can obtain.

Traffic and Health Charts

Reports	Description	How to Use
Popular URLs Popular Services Popular Domains	Provide information on application areas that receive maximum amounts of traffic	Optimize areas for best performance and scale
Worst-Behaving URLs Worst-Behaving Services Worst-Behaving Domains	Provide information on applications areas that show maximum response times	Debug these areas using per-request analysis and improve performance
Response Codes	Provide information on response codes being returned to the clients	If more errors (4xx and 5xx) are seen, debug using per-request analysis and fix
Secure vs. Open SSL Connection SSL Time	Show what part of the application is exposed without SSL, unsuccessful SSL connection attempts and the average time of SSL negotiation	If any SSL performance parameter goes beyond expectation, selected SSL protocols, ciphers and certification need to be checked;
Connections	How many client connections are coming to A10 Lightning ADCs (front-end) and how many connections are created by A10 Lightning ADC to server (back-end)	For high traffic, the difference between front-end and back-end connections should be high. If not, check server's connection closing settings for reducing load on server
End-to-End Response Time	Various charts displaying how much time is consumed in various portions of request-response flight	Optimize the portion of flight where maximum time is being spent
Per-Server Health Charts CPU Utilization Average Latency Connection Errors Response Codes	Charts displaying various health metrics for the application server	If any metrics goes beyond the limit, debug the server and fix

Security Charts

Reports	Description	How to Use
Top Threats	Quick glance of potential threats to the application along with their volume	Get detailed analysis if a real threat exists
Per-Client WAF Events	Multiple charts displaying suspected WAF attacks from clients	Analyze using per-request analysis; block the client if it is an attack or create exception rule
Threats Trend	Trend charts showing pattern of potential attack	Take security measures according to the trend and be prepared for the time
Blocked Cookies	Lists the cookies blocked as per policy; cookies blocked for maximum number of times remain on the top	Fine-tune cookie security policy
Session Tracking	Trend of new, active, blocked sessions	Fine-tune rate-limiting or scale the infrastructure accordingly
Surge Protection	List of clients involved in slow communication and resource hogging	Fine-tune surge protection policy
Surge Queue	Trend of request-queue length at the time of traffic surge	Scale infrastructure if queue is visible most of the time

Per Requests Analysis

Reports	Description	How to Use
Logs	Access logs for each request, along with details of request size, response size, source and referrer info, info of the server served the request along with time taken in each portion of the transaction	Get to root of the problem and pinpoint problem area

Alerts

Reports	Description	How to Use
Average CPU Utilization	CPU utilization of application servers	Typically occurs because of change in load/traffic; scale the infrastructure accordingly
Sum Network In	Total size of the requests	Find out if someone is trying to upload a large amount of data; may be an attack
Sum Network Out	Total size of responses	Find out if someone is trying to download a large amount of data; may be a data theft
App Server Errors (Count)	Error responses from application servers	Debug the servers for errors; may also be a scan for an attack
WAF Events (Count)	Number of events in WAF per applied policy	Check for attack or false positives and block or tune the policy
App Server Monitoring	If an application server is responding or not	Check the application server for health and fix
App Server Error Percentage	What portion of traffic is resulting in error	Debug the server when errors become disproportionately high
App Server Connection Errors (Count)	App servers failure for TCP connections	Debug the application server for health or scale the infrastructure
App Server Latency	Response time from app servers	Debug the app server for response time or scale the infrastructure
App Sever Pending Requests	Requests in the queue to be accepted	Debug the app server or scale the infrastructure

System Requirements

A10 Harmony Controller: SaaS Model

Available as a service, the SaaS-based controller subsystem is fully managed and monitored by A10. The Controller is hosted and service provided from data centers in the United States. It is built on top of a hardened operating system, installed on one or more high-performance, industry-standard servers and hosted at a public cloud provider.

The controller is in an isolated environment with network-layer ACLs and access is granted only to authorized personnel. Data exchanges within the sub systems are encrypted using strong ciphers and sensitive data like passwords; SSL private keys are stored in the database with strong encryption. External access is always through industry-standard SSL communication.

The A10 Networks team runs regular security scans and audits for security vulnerabilities. In short, the controller offers multiple layers of security that are reviewed to ensure security and compliance.

A10 Harmony Controller: Self-Managed Model

The Harmony Controller may be optionally obtained as a software license under the full management and control of the organization. In this case, the controller may be flexibly deployed in on-premise data centers, private clouds or public clouds, including Amazon Web Services (AWS), Microsoft Azure or Google Cloud Platform.

The communications and security aspects operate similar to the SaaS model described above. For detailed system requirements refer to the A10 Harmony Controller datasheet.

A10 Lightning ADC

A10 Lightning ADCs may be deployed in AWS, Azure or Google cloud platforms natively and in any other platform using Docker containers. Deploying A10 Lightning ADCs in the same subnet as application servers is the best practice. It is recommended to deploy a minimum of two instances for high availability.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com.**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DS-15121-EN-02
Apr 2017

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Hong Kong
hongkong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
southasia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at **a10networks.com/contact** or call to speak with an A10 sales representative.