IBM Edge Delivery Services

Service capabilities

Get started

IBM

How to use this doc:

IBM Edge Delivery Services, powered by Akamai, solves web-based security and performance challenges that all businesses encounter by addressing problems inherent to the Internet (slow, unreliable, not secure). Following that theme, in this ebook, we have sorted the capabilities of IBM Edge Delivery Services under either the security category or the performance category.* Where applicable, we have listed analyst reports that feature Akamai.

Category	Product name	Analyst report
Security	Bot Manager	The Forrester Wave: Bot Management, Q3 2018
	Enterprise Application Access	The Forrester Wave: Zero Trust eXtendedEcosystem Providers, Q4 2019
	Enterprise Threat Protector	
	Kona Site Defender	Gartner Magic Quadrant for Web Application Firewalls -September 2019
	Web Application Protector	The Forrester Wave: DDoS Mitigation Solutions, Q4, 2017
Performance	CloudTest/ mPulse	
	Dynamic Site Accelerator	
	Fast DNS	IDC MarketScape Worldwide Commercial CDN 2019
	Global Traffic Management	
	Ion	IDC MarketScape Worldwide Commercial CDN 2019

*Not a comprehensive list of the capabilities of the IBM Edge Delivery Services portfolio.

Introduction

Introduction

IBM Edge Delivery Services is a set of services that can improve the security, availability, and performance of your Internet-accessible web and mobile applications. It works on any web-connected device at any time, regardless of where the applications are hosted, all without changes to hardware and software in your data center. It transforms the Internet into an enterprise-class security and delivery platform for your users and applications.

IBM Edge Delivery Services delivers 100 percent of customer site traffic through a global platform of servers distributed all over the Internet in over 3,900 locations—spanning more than 230,00 network servers across more than 130 countries.

IBM Edge Delivery Services helps protect and accelerate your applications and enterprise network with the following capabilities:

Protect and secure

- Bot Manager
- Enterprise Application Access (EAA)
- Enterprise Threat Protector (ETP)
- Kona Site Defender
- Web Application Protector

Accelerate performance

- Dynamic Site Accelerator
- CloudTest/mPulse
- Fast DNS
- Global Traffic Management
- Ion

Bot Manager

Enterprise Application Access

Enterprise Threat Protector

Kona Site Defender

Web Application Protector

Bot Manager

Overview

Not all bots are created equal some are helpful, most are a nuisance and others harm your business by leading to account takeover and fraud. Regardless of the business impact, bot traffic can reduce website performance for legitimate users and increase IT costs. Traditional bot mitigation tools typically only block bot traffic, impacting beneficial and harmful bots alike while prompting bots to evolve and return better hidden from detection. Organizations need a solution that can better manage their interaction with different types of bots and the impact they have on the business and IT infrastructure.

Bot Manager delivers advanced bot detection to spot and avert the most evasive threats keeping even the most sophisticated bots away from your business. Bot Manager provides organizations with a flexible framework to better manage the wide array of bots accessing their websites every day. It offers the abilities to identify bots as they first arrive, categorize them and apply the most appropriate management policy for each category. This allows greater control over how each organization interacts with different types of bots, maximizing business benefits while reducing any negative business or IT impact.

Benefits to your business:

- **Controls** the wide range of automated bot traffic — both good and bad — interacting with your website
- **Helps gain visibility** into the amount and characteristics of bot traffic attempting to access your website
- **Helps maintain a competitive advantage** and retain control over customer relationships by preventing price and content scraping

Continued... →

Bot Manager

Enterprise Application Access

Enterprise Threat Protector

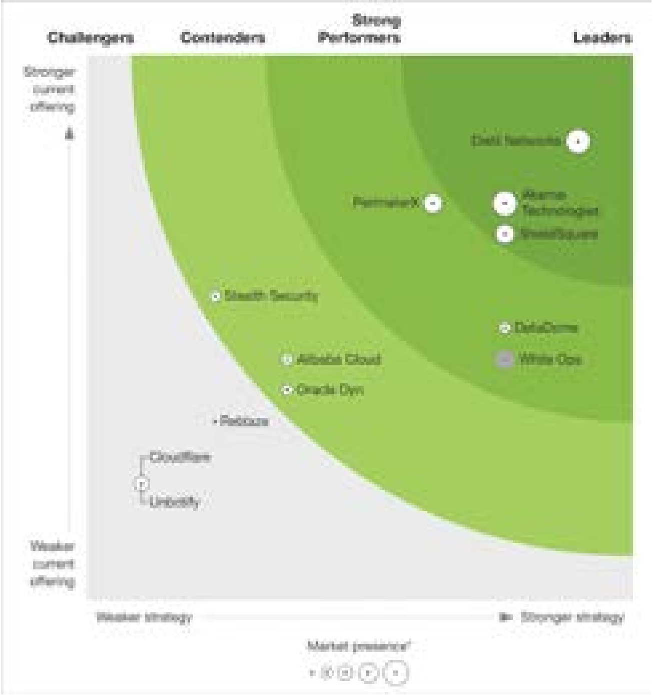
Kona Site Defender

Web Application Protector

How it works

Bot Manager combines the visibility and scale of Akamai's globally distributed platform with bot-specific capabilities to identify, categorize, manage and report on bot traffic. Clients — real users and bots — connect to your web application through the most optimal Akamai server, and Bot Manager detects, identifies and manages bots at the edge, before they get to your applications or data centers.

Bot Manager is designed to take configured actions on bot activity at the edge server, forwarding only clean traffic to the origin. You have the flexibility to manage identified bots individually or create categories of bots, assigning different management policies based on the desired interaction with each bot category. Bot Manager helps organizations better understand their bot traffic through the Security Center dashboard and built-in Bot Activity and Bot Analysis reports.



The Forrester Wave: Bot Management, Q3 2018

Benefits to your business:

- **Reduces financial risk** by protecting against credential abuse, card balance checking, and other forms of web fraud
- **Lowers costs** by slowing the growth of your web infrastructure and reducing the IT overhead required to manage bots yourself
- **Improves user experience** by reducing the impact of bots on the web infrastructure during regular business hours

Enterprise Application Access

Overview

Increased mobility and a growing utilization of the cloud have driven the need to monitor, control and secure access to enterprise applications without hindering workforce productivity. Enterprises must also deal with the risky proposition of providing access to a varied list of contractors, suppliers, partners, customers and developers. Regardless of where these applications are hosted—whether in a public cloud or private data center—this is a complex, cumbersome task requiring on-premises hardware and software such as application delivery controllers (ADC), virtual private networks (VPN), identity and access management (IAM) systems, and more. Yet with all of these technologies, enterprises are still exposed to a variety of security risks stemming from the fact that access to internal applications opens up the entire network to attack.

Enterprise Application Access provides a simple, secure and fast alternative to traditional access technologies such as VPN, remote desktop protocol (RDP) and proxies. With Enterprise Application Access, applications are hidden from the Internet and public exposure. It enables a zero-trust architecture by closing all inbound firewall ports, while also providing identity and authentication for users so that access is granted to only those specific applications required by a given role, and not to the entire network stemming from the fact that access to internal applications opens up the entire network.

Benefits to your business:

Drastically improves your security posture by enabling a zero-trust architecture

- Keeps all users off of your network with application-level access vs. network-level access
- Locks down your firewall or security group to all inbound traffic
- Makes your application IP addresses invisible to the Internet
- Easily adds MFA to any application with the click of a button

Reduces complexity for IT

- Seamless SSO across all applications, whether they’re on-premise, IaaS, or SaaS
- Consolidates ADCs, WAN optimization, VPN, and MFA
- No internal hardware or network changes required, such as firewall rules, IP address whitelisting, etc.

Continued... →

Bot Manager

Enterprise Application Access

Enterprise Threat Protector

Kona Site Defender

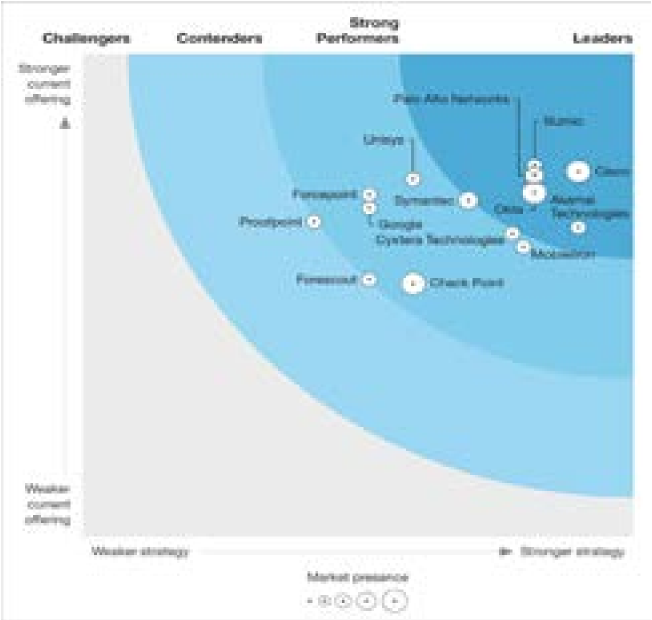
Web Application Protector

How it works

Enterprise Application Access provides secure access-as-a-service that eliminates the need to punch holes in the network perimeter. Instead, users access applications through the cloud, which stops and secures user access far outside your network. With Enterprise Application Access, there is no direct path into your applications; the solution dials out a secure, mutually authenticated transport layer security (TLS) connection from within your network or cloud and brings the application to the user.

No tunnels mean that there is no direct path for malware to land inside your network and potentially spreadto sensitive or privileged systems. All user connections are stopped in the cloud, terminating on secure proxies while applying strong authentication and security controls. You can add your own security controls for increased protection across all sensitive applications.

Enterprise Application Accessmakes accessing applications fast and intuitive for end users, and reduces support calls for poor application performance, VPN connectivity issues and device incompatibilities.



The Forrester Wave: Zero Trust eXtended Ecosystem Providers, 4Q 2019

Reduces complexity for IT

- Users access applications from any device — without any additional software, including VPNs and browser plugins
- Stands up new applications and provisions users in minutes
- Automatically integrates with other zero trust ecosystem security solutions

Provides a fast, seamless user experience

- Complete auditing and reporting of user activity
- Available as built-in reports or can be integrated with your existing tools
- Eliminates multiple passwords and provide application access through a single web portal
- Reduces latency for higher application adoption and fewer IT help desk ticket requests
- Delivers applications to any device type, anywhere in the world, with a consistent user experience

Bot Manager

Enterprise Application Access

Enterprise Threat Protector

Kona Site Defender

Web Application Protector

Enterprise Threat Protector

Overview

As organizations adopt Direct Internet Access (DIA), SaaS applications, cloud services, mobility, and the Internet of Things (IoT), their attack surface increases dramatically, and they are faced with a host of new challenges. Protecting the organization and users against advanced targeted threats such as malware, phishing and data exfiltration becomes exponentially more difficult. Security control-point complications and complexities and security gaps in legacy solutions have to be managed.

Enterprise Threat Protector (ETP) is a Secure Internet Gateway (SIG) that enables security teams to ensure that users and devices can securely connect to the Internet wherever they happen to be, without the complexities associated with other legacy security solutions. Enterprise Threat Protector is powered by real-time threat intelligence based on global insights into Internet and DNS traffic.

It leverages real-time cloud security intelligence and Akamai's proven, globally distributed platform to proactively identify and block targeted threats such as malware, ransomware, phishing, and DNS-based data exfiltration. The ETP portal enables security teams to centrally create, deploy and enforce both unified security policies and acceptable use policies (AUPs) in minutes for all employees, wherever they are connected to the Internet.

How it works

Enterprise Threat Protector uses multiple layers of protection — DNS, URL, and inline payload analysis — delivering optimal security and reducing complexity, without impacting performance.

Benefits to your business:

- **Improves security posture everywhere** Adds a layer of security that uses DNS as a control point to uniformly and immediately block malicious domains and communications for all of your users, whether they are on or off network
- **Secures DIA connections** Protects your branch DIA traffic quickly with zero complexity, without replicating your security stack at every location
- **Protects guest Wi-Fi** Easily enforces an acceptable use policy (AUP) across your guest Wi-Fi for both brand and user protection

Continued... →

Bot Manager

Enterprise Application Access

Enterprise Threat Protector

Kona Site Defender

Web Application Protector

By simply directing your external recursive DNS traffic to Enterprise Threat Protector, all requested domains are checked against real-time domain-risk-scoring threat intelligence. Users are proactively blocked from accessing malicious domains and services while requests to safe domains and services are resolved As this validation happens before the IP connection is made, threats are stopped earlier in the security kill chain. In addition, DNS is effective across all ports and protocols, thus protecting against malware that does not use standard web ports and protocols.

Domains that are considered risky based on threat intelligence data are automatically forwarded to a cloud proxy on our platform. The requested URL is checked against URL threat intelligence, and malicious URLs are automatically blocked. The proxy inspects both HTTP and HTTPS URLs.

The HTTP and HTTPS payloads from risky domains are then scanned in real time using multiple advanced malware-detection engines. These engines use a variety of techniques—including signature, signatureless and machine learning—that deliver comprehensive zero-day protection against potentially malicious files, such as executables and document files, as well as other malware that is embedded directly into the requested web page, such as obfuscated malicious JavaScript.

Enterprise Threat Protector easily integrates with other security products and reporting tools, including firewalls and SIEMs, as well as external threat intelligence feeds, allowing you to maximize investments across all layers of the enterprise security stack.

Kona Site Defender

Overview

In order to thrive in today's fast-moving and hyper-connected digital economy, your business applications are designed to be highly accessible through websites and APIs by consumers and business partners. However, they also offer an attractive entry point to access valuable data and therefore are the main target of serious attacks.

Kona Site Defender provides broad protection for websites and applications from downtime and data theft caused by opportunistic and sophisticated web attacks and DDoS attacks. Organizations that use Kona Site Defender are able to aggressively innovate their web offerings to increase delivery performance without the distraction of increasing targeted attacks.

Benefits to your business:

- **Protects** revenue, customer loyalty, and brand equity
- **Maintains** application performance even when under attack
- **Reduces** cost from spikes in attack traffic
- **Provides** advanced integration with IT infrastructure and DevOps
- **Leverages** best-in-class application security experts
- **Provides** deep threat insight visibility with web security analytics

Continued... →

Bot Manager

Enterprise Application Access

Enterprise Threat Protector

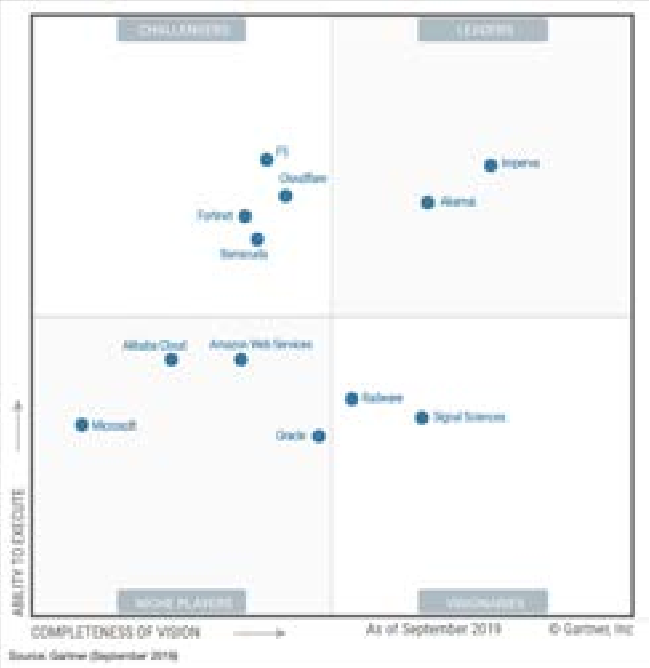
Kona Site Defender

Web Application Protector

How it works

Kona Site Defender runs on Akamai's Intelligent Platform, providing the resiliency and availability for you to deliver superior online experiences, even when under attack. Online traffic connects to your web application through the most optimal edge server, which drops network-layer DDoS attacks instantly.

Automated rate controls block application traffic that exceeds your defined thresholds to defend against application-layer DDoS attacks. Kona Site Defender inspects web traffic and API requests using proprietary web application firewall (WAF) rules with high accuracy. Optional Client Reputation Service allows you to increase the level of protection by blocking traffic originating from clients with recent malicious behavior, and you can add DNS layer protection with Fast DNS.



Source: Gartner (September 2019)

Gartner Magic Quadrant for Web Application Firewalls - September 2019

Continued...

Web Application Protector

Overview

Securing your web applications can be a daunting task. Even the most seasoned security professionals can find it challenging to keep up with the latest threats, understand what really matters to you and your applications, and update your security protections in a timely manner. For organizations without dedicated staff and expertise, deploying and managing a WAF and DDoS protection solution effectively over time can be even more challenging.

Web Application Protector combines an easy-to-manage WAF with highly scalable DDoS protection in a single cloud-based solution. Web Application Protector can help protect your applications from a wide range of network-and application-layer threats with less effort and overhead — whether they are located in your data centers or in the cloud. In addition, Web Application Protector is built on Akamai's Intelligent Platform and comes with built-in performance capabilities, helping provide security without compromise.

Benefits to your business:

- **Deploys quickly**
  Configures Web Application Protector's security protections in just a few clicks to get your applications protected faster.
- **Enables easy management**
  Helps continuously and transparently updates the included security protections with no human intervention required, to protect your application with less effort.
- **Operates more securely online**
  Protects your applications from DDoS and web application attacks to reduce the risk of downtime and data theft and operate more securely online.

Continued... →

Bot Manager

Enterprise Application Access

Enterprise Threat Protector

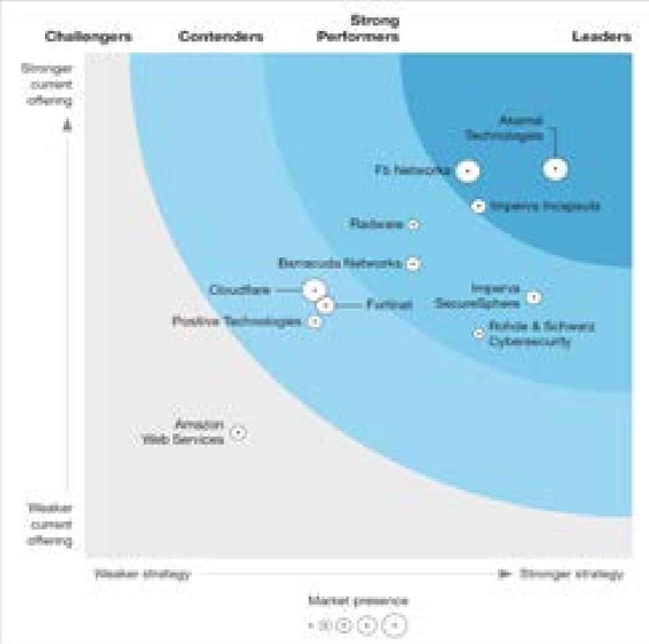
Kona Site Defender

Web Application Protector

How it works

With Web Application Protector, clients connect to your web applications through the closest edge server. Every server inspects web traffic to detect and block DDoS and web application attacks, while delivering web content to legitimate users. With more than 230,000 servers around the world, Web Application Protector has the scale to stop the largest attacks — at the edge, before they reach your applications.

Web Application Protector simplifies the task of securing your applications with automated updates to included security protections. With visibility into attacks against thousands of IBM Edge Delivery Services clients, advanced machine learning algorithms continuously refine these protections — and transparently update your configuration without requiring any human intervention.



The Forrester Wave: Web Application Firewalls, Q2 2018

CloudTest/mPulse

DynamicSite Accelerator

Fast DNS

Global Traffic Management

Ion

CloudTest/mPulse

Overview

CloudTest is a large, highly scalable global load testing platform. It allows you to safely simulate your largest events in production with precise control, while producing a live analysis of what your site or app is capable of on your busiest day, and helping you drill down to the source of any performance bottlenecks.

CloudTest delivers tests of infinite scale through the cloud as well as load testing inside a pre-production environment. Testing capabilities include web and mobile apps, APIs, databases, and webservices, all with full support for continuous integration. Real-time analytics and customizable dashboards provide actionable intelligence, allowing for root-cause analysis while tests run. With real-user monitoring capabilities from mPulse, CloudTest allows for virtually the most realistic and accurate testing in any environment.

How it works

CloudTest, at its core, has one of the most sophisticated analytics engines, which allows for load testing with millions of users—simultaneously taking billions of data points and presenting them in real-time to give you actionable intelligence. With features like Dynamic Ramp, you have a real-time, interactive way to test the limits of your site or application. Waterfall dashboards allow you to isolate the elements on the page that are impacting your application. Analyzing your data while the test is running has proven to reduce brake-repair cycles, delivering the actionable intelligence you need to ensure online success.

Benefits to your business:

Test faster: Test quickly and efficiently with real user scenarios so you can quickly isolate bottlenecks and fix problems.

Scale: Spin up larger loads with broader geographic reach than most other test solutions, with no limits on real-time analytics processing of test results or user performance data.

Stay in control: Test in production safely with real time results and the ability to ramp load up or down instantly.

Continued... →

CloudTest/mPulse

DynamicSite Accelerator

Fast DNS

Global Traffic Management

Ion

Engineer better releases with a solution designed to help you continuously test throughout your entire lifecycle—from development to staging to production. Developers can test their API services, Dev/QA can automate with continuous integration, and then performance teams can test at scale, all with the same test. Conduct performance tests in your pre-production environment, or leverage CloudTest's patented real-time analytics to test at scale in production. Once code is deployed to production, measure your real users with mPulse. With CloudTest, you can use path analysis, abandonment rates, and conversion metrics to build better tests for your next release.

Dynamic Site Accelerator

Overview

Customers browsing and buying online expect instant gratification and an experience that is increasingly more entertaining and personalized, with offers designed specifically for them. Delivering on this expectation requires rich, interactive content and applications that are generated dynamically. But the very innovations that make these experiences so engaging also slow page downloads and put the customer experience at risk.

Rendering pages on the fly can lead to delays and failures in content delivery, causing online customers to simply abandon the site. To avoid site abandonment, your websites must deliver superior performance to every customer, scale to handle high traffic loads during peak usage periods and maintain around-the-clock availability.

Dynamic Site Accelerator gives you performance up to five times faster than your original web infrastructure and handles the specific requirements of dynamically generated content—without a costly hardware build-out. It speeds-up and secures highly interactive websites and provides visibility and intelligence on usage, visitors and online activity.

How it works

Dynamic Site Accelerator is built on Akamai's global cloud platform and is designed to improve the performance, scale and security of web experiences delivered over the public Internet. It extends your company's existing data and application infrastructure so you can deliver fast, high-quality web experiences regardless of how, where and when end-users choose to connect. Dynamic Site Accelerator's layered approach to scale, performance and intelligence is backed by our industry-leading performance and availability service level agreement.

Benefits to your business:

Reduced IT costs: Increases scalability and origin offload, leveraging the power of the highly distributed Akamai cloud delivery platform

Reliable, secure and improved web experiences: Continuously and transparently applies real-time network optimizations and advanced caching techniques to deliver reliable, fast, and secure content

DevOps automation: Reduces time to market more by automating your DevOps workflows—deploying new properties with streamlined and simplified onboarding, configuration, and monitoring

Fast DNS

Overview

Despite its importance to website and application performance, many organizations under-deploy domain name system (DNS) infrastructure, often relying on just two or three DNS servers. This approach leaves them vulnerable to data center outages as well as DDoS attacks.

Fast DNS is a cloud-based DNS solution that delivers around-the-clock DNS availability, improves DNS responsiveness and provides the resilience to defend against even the largest DDoS attacks. Built on a globally distributed anycast network, it can be implemented as a primary or secondary DNS service, replacing or augmenting existing DNS infrastructure as needed.

How it works

Fast DNS Leverages Akamai's Intelligent Platform, with thousands of DNS servers in hundreds of points of presence worldwide, to provide a high level of DNS service availability. Fast DNS comes with a 100 percent uptime service level agreement (SLA); providing you with confidence that your customers and employees can connect to your website and application servers.

It directs users to a high-performing DNS server based on network conditions to improve responsiveness of your DNS infrastructure. The globally distributed anycast network accelerates DNS resolutions for users connecting to your sites and applications from anywhere in the world.

Benefits to your business:

- **Around-the-clock availability**
  Ensures around-the clock availability by leveraging Akamai's scalable, globally distributed platform
- **Faster, more reliable web experiences**
  Achieves faster performance with zone apex mapping and thousands of servers worldwide
- **Defense against DDoS attacks**
  Protects your online business from the effects of DNS-based DDoS attacks and other threats
- **Reduced costs**
  Helps reduce costs with pricing based on the number of zones, not requests

Continued... →

CloudTest/mPulse

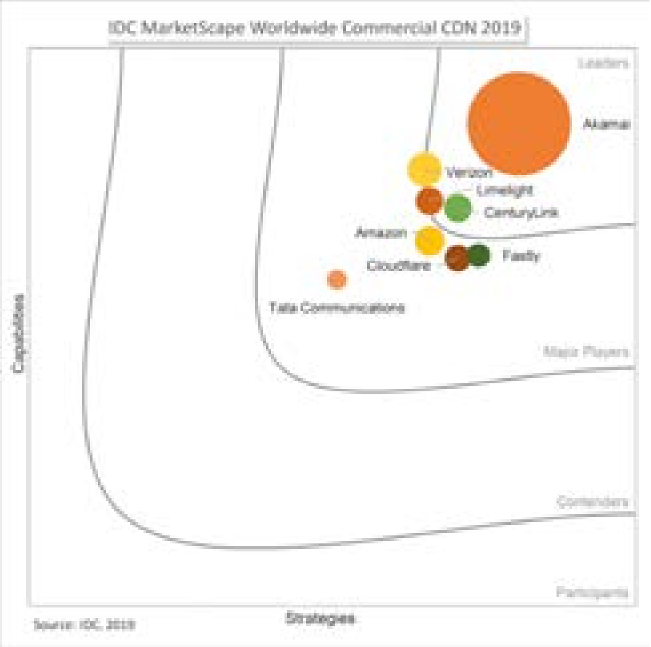
DynamicSite Accelerator

Fast DNS

Global Traffic Management

Ion

At the same time, it protects you against DDoS attacks targeting the DNS infrastructure to disrupt websites and application servers. Fast DNS provides a highly scalable DNS platform with sufficient capacity to absorb even the largest DDoS attacks while responding to legitimate user requests, so you can maintain user access to faster online experiences even when you are under attack.



IDC MarketScape Worldwide Commercial CDN 2019

CloudTest/mPulse

DynamicSite Accelerator

Fast DNS

Global Traffic Management

Ion

Global Traffic Management

Overview

Achieving high application availability and optimal online response times can involve a variety of site implementation strategies including geographically diverse data centers and redundant network architectures and components. Most often, traditional hardware load balancing appliances alone can fall short, as they do not account for Internet bottlenecks that can affect an end-user's ability to connect to an appropriate data center.

Global Traffic Management, built on Akamai's cloud delivery platform, is a DNS-based load balancing solution that balances traffic across all data sources—both cloud-based and on-premises infrastructures. It provides you a highly scalable, fault-tolerant load balancing solution that ensures high performance and availability under any peak demands.

How it works

Global Traffic Management is designed so that Internet users can more reliably get to your websites or any other IP application. It applies an Internet-centric approach to global load balancing to provide high site availability and responsiveness to online user requests. Unlike traditional hardware-based solutions that reside within the data center, Global Traffic Management is a fault-tolerant solution that makes intelligent routing decisions based on real-time data center performance health and global Internet conditions. It's the only load balancing solution that leverages the scale and speed of Akamai's globally distributed Intelligent Platform.

Benefits to your business:

- **Reduces IT cost and complexity** by offloading to the Akamai Intelligent Platform and standardizing optimization across all applications
- **Improves response time and mitigates traffic impact** by addressing real-time Internet conditions
- **Optimizes site availability** so users can always reach your applications and site by improving load balancing
- **Modifies web traffic allocation and new property set-up dynamically** through greater network visibility and control
- **Increases service availability** and helps avoid potential security threats with built-in reliability and redundancy

Ion

Overview

The pressure to deliver great online experiences is higher than ever. To realize digital success, every business must provide a consistently great experience on every channel and device. However, organizations looking to provide safe, reliable and fast online experiences often lack the tools and capabilities to manage all aspects of end-to-end delivery over the Internet. With all of these challenges, bringing differentiated solutions to market in a timely fashion can become increasingly difficult, and threaten revenues and customer loyalty.

Ion is a suite of integrated performance optimizations, tools and intelligence that together address each stage of delivering compelling online experiences—from development and deployment, through middle-mile and cellular networks, to user devices, browsers and apps.

Built on the SLA-backed bedrock of Akamai's global cloud delivery platform, Ion allows businesses to deliver fast, contextually aware experiences that adapt to each user and help drive increased impressions, conversions and brand equity.

Benefits to your business:

- **Accelerates content** by routing around congestion points and other bottlenecks, while leveraging the latest network protocols to accelerate dynamic content
- **Engages more users** by providing all users with the same experience regardless of their device, network, or geographic location. Targets audiences with the best possible experience for each of them
- **Helps gain valuable insights** to drive better experiences and improve your business. Applies performance optimizations automatically based on real user and application behaviour

Continued... →

CloudTest/mPulse

DynamicSite Accelerator

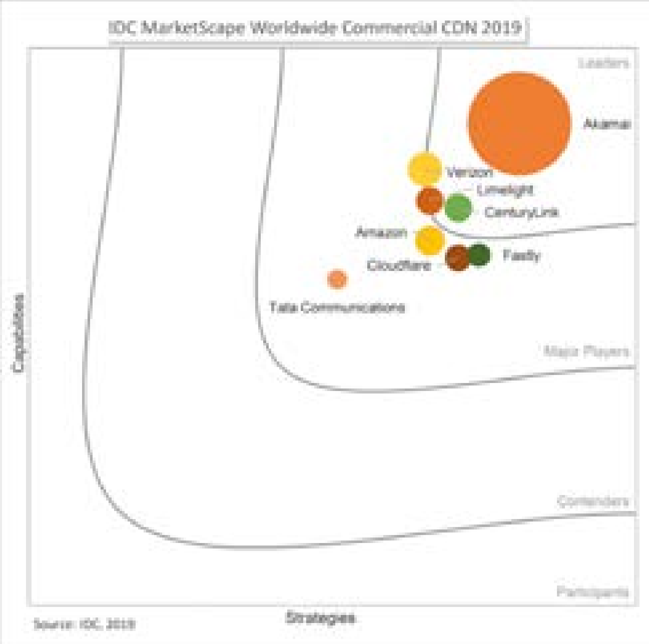
Fast DNS

Global Traffic Management

Ion

How it works

Ion helps every user have a seamless experience across different device types and network conditions, however they choose to connect, adapting in real time to changes in content, user behavior and connectivity. Ion combines the scalability of Akamai’s global content delivery platform with the fastest dynamic content acceleration. It also enables cellular optimizations designed to lower latency and avoid disrupting user engagement. With Ion, you can rapidly onboard, manage, and tune digital properties. Once on the platform, Ion enables you to craft the differentiated solution your users demand with a powerful set of integrated capabilities.



IDC MarketScape Worldwide Commercial CDN 2019

Benefits to your business:

- **Delivers enhanced experiences** by creating the ideal mobile experience using insight into your users devices, and tools to overcome the challenges of cellular networks
- **Reduces page weight and accelerates rendering** by reducing resources and only sending necessary bytes to users, so pages load faster
- **Decreases operational costs while gaining** reliability by reducing the load on your origin infrastructure, especially during peak demand periods

Why IBM Edge Delivery Services?

We make the Internet fast, reliable and secure. Our comprehensive solutions are built on Akamai's globally distributed Intelligent Platform, managed through a unified, customizable control center for visibility and control, and implemented by professional services experts who get you up and running easily and support your strategies for innovation and growth.

For additional information on IBM Edge Delivery Services, visit **ibm.biz**/services-edge.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
January 2020

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.