section.io

Comparison Sheet: section.io and Akamai

Akamai was at the forefront of the Content Delivery industry when they began serving content from global servers (PoPs) in the 1990s. By bringing content closer to end-users and caching certain objects such as static images, Akamai was able to reduce load on website servers and serve content to visitors more quickly.

While section.io and Akamai both rely on a network of servers with reverse proxies installed, the way the two networks are built and how developers work with each platform to configure and test settings are dramatically different. This paper will go over the major differences in architecture, reverse proxy choice, and configuration options between the two.

QUICK FACTS

Feature	Akamai	section.io
Global delivery network	Thousands of Global PoPs of varying ages.	24 modern "Super PoPs"
Caching/Performance	Static, Dynamic and HTML doc caching	Static, Dynamic and HTML doc caching
Security	Traditional WAF and bot blocking	Choice of Traditional WAF or Intelligent WAF plus future security-focused proxies.
Reverse proxy choice	No choice of reverse proxies, Black boxed proprietary versions of Squid for caching, ModSecurity WAF plus blaze.io for FEO.	Choice of WAFs ,current versions of Varnish Cache, Google's PageSpeed, OpenResty, Nginx, and more being released.
Configuration options	Basic changes with portal obfuscating proxy config. Professional Services needed for complex configuration changes.	Full software level control over configuration provided in section.io portal with git backed workflow.
Metrics and Diagnostics	Metrics in portal. FTP log shipping hourly.	Unlimited timespan metric access in portal or open end point querying. Realtime enriched logs available in Kibana interface with open endpoints for external system querying..

Feature	Akamai	section.io
Development Integration	Not offered	Full, software backed application development cycle integration.
Pricing	Not publicly available. Minimum 1 year contracts. Additional costs for SSL, professional services	Monthly pricing with no long term commitment. Single Proxy: $149.95/month for 1,000,000 page views plus unlimited additional pages at $0.25/1000 Multiple Proxy: $499.95/month for 1,500,000 page views plus unlimited additional page views at $0.45/1000. Includes SSL certs, DNS hosting, HTTP/2.

DETAILED INFORMATION

Introduction

Choosing a Content Delivery solution is an important decision for global businesses who rely on their website for revenue and can't afford downtime or slow page speeds. When choosing between Content Delivery solutions businesses need to consider many factors including:

What your website is looking to improve through a CDN - performance, security, or both.

What type of CDN will work for your developers.

What CDN is right for your website or application and the platforms it runs on.

The cost structure of different CDNs.

section.io and Akamai both offer website performance and security benefits built on the backbone of global server networks, however the way these benefits are reached is considerably different.

In this paper we go through the core differentials between section.io, a flexible Content Delivery Grid built to integrate with modern development processes, and Akamai, one of the first and the largest Content Delivery Network available.

Network Architecture and PoPs

All Content Delivery solutions consist of two main layers: A DNS layer which finds the server closest to the end-user from a global server network, and a reverse proxy layer which acts on behalf of your website server and injects additional security and performance functions, such as caching content.

When Akamai first started in the 1990s, the DNS layer and server network were incredibly important, as most of the speed benefits associated with using a CDN came from serving content from a server that was much closer to end-users than the website's origin server. Using distributed servers also reduced the load on those website origin servers, preventing them from slowing down or going offline due to a influx of traffic.

Over the years, Akamai has grown its global server network to over 200,000 servers or Pointsof Presence (PoPs) around the globe. This gives Akamai the largest server network of any Content Delivery solution. However, the architecture of many of these servers is now outdated.

More modern Content Deilvery solutions such as section.io rely on fewer, newer "Super PoPs" that are more powerful than Akamai's PoPs and are strategically placed along the Internet backbone so they can still deliver content quickly even if it is coming from a furthur distance.

section.io currently has 24 modern PoPs located throughough the Americas, Europe, Asia, and Australia. In building its Content Delivery Grid, section.io has focused on providing users with the ability to cache more content through a highly configurable reverse proxy layer, and to deliver a higher cache hit rate. When considering the number of PoPs your website needs, you should think about:

1. Where your visitors are located.

2. How often you will be able to fill cache of each server in your Content Delivery solution.

While more PoPs can sound appealing, a large volume of PoPs can actually be detrimental to your website speed if the PoP caches are not being filled regularly.

If visitors are directed to PoPs that have not been recently filled by a prior visitor, they will bypass the PoP and go to your website origin server, resulting in a cache miss. The more PoPs, the higher likelihood visitors will be directed to an empty PoP cache.

In reality, the vast majority of websites have visitors from concentrated geographical areas and therefore only use a small fraction of the globally available PoPs offered on Akamai.

In addition, the speed benefits offered by closer PoPs are often outshined by the website performance improvements that can be gained by caching a larger amount of content, as we explain in the next section.

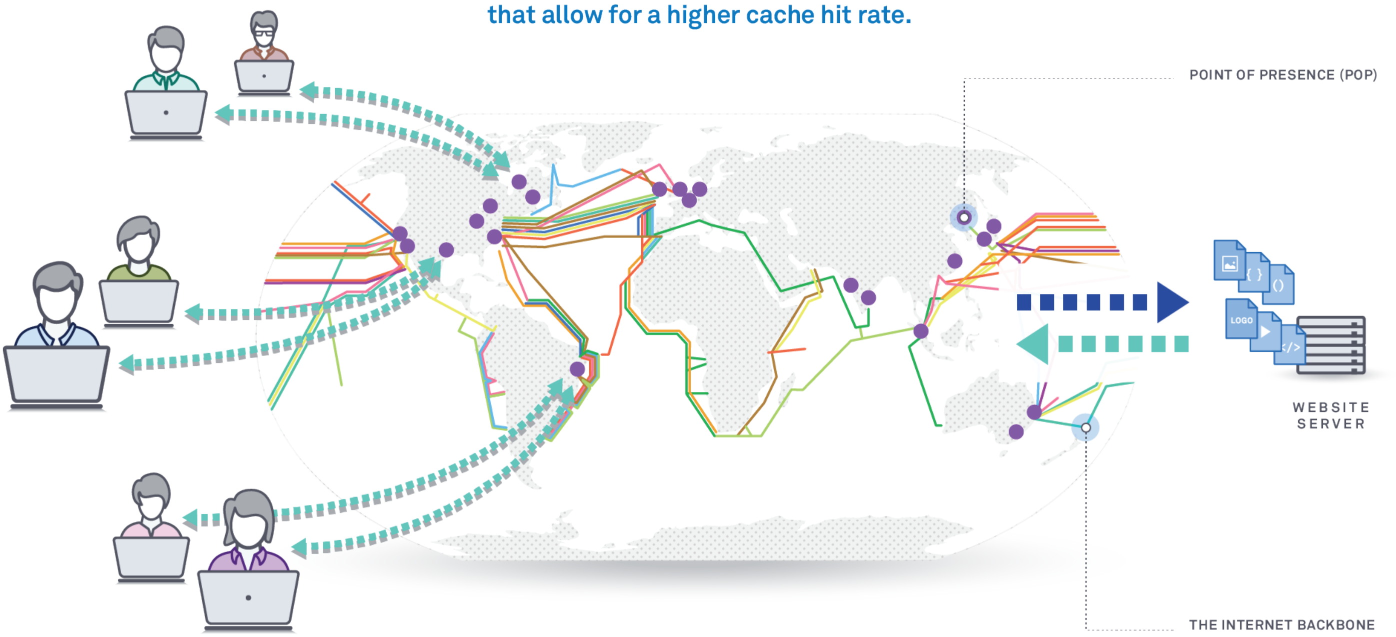
Website Performance Features

As noted in the prior section, Content Delivery solutions consist of a DNS layer and reverse proxy layer. It is the reverse proxy layer that caches content, blocks malicious traffic, and provides other speed and security benefits.

In terms of performance improvements, caching is the main way Content Delivery solutions are able to speed up page load time.

By caching or storing content on global servers, Content Delivery solutions can serve end-users from the cache without going back to the website server, saving time and reducing stress on the origin server.

Modern CDNs have fewer, more powerful PoPs that allow for a higher cache hit rate.



section.io and Akamai both run caching reverse proxies as part of their Content Delivery solution. section.io offers a choice of unmodified Varnish Cache versions, while Akamai uses a custom caching solution which is likely a modified version of Squid.

Both Varnish Cache and Squid can easily cache static objects such as images, documents, and other files which do not change often. However, Varnish Cache excels when caching dynamic content including stylesheets, JavaScript, and even full HTML documents.

This is important as more websites have a large amount of dynamic content which websites should aim to cache. By caching the HTML document, which is the first piece of information a browser receives from the server, the Time To First Byte will be significantly reduced.

section.io and Akamai also differ in the way they offer caching reverse proxies and how they are configured. section.io allows developers to choose Varnish v3, v3 with Magento Turpentine, or v4. The Varnish versions are unmodified so developers can troubleshoot using open-source docs, and the section.io platform provides an interface to set up basic caching and a repository where advanced configurations can be made directly.

Akamai does not disclose the exact reverse proxy used in their CDN, and advanced configurations may require support from an Akamai specialist. Because the reverse proxy is not open-source, troubleshooting when issues arise can be more difficult.

section.io provides additional performance benefits by serving all HTTPS traffic over over HTTP/2, the updated and faster version of the HTTP communications protocol.

Website Security Features

Akamai and section.io both provide some included security features and the option to add a Web Application Firewall to your website. Next is a breakdown of the differences in security offerings from section.io and Akamai.

Core Security Features

All Content Delivery solutions include some protection from attacks: By taking away traffic from your origin server and serving content from global caches, you are already more able to withstand an attack than you would be if all traffic was going directly to your origin server. Therefore, the amount of content you can cache and the cache hit rate you achieve should be considered when thinking about the security of your Content Delivery solution.

Another important element of website security is serving traffic over the HTTPS encryption protocol, which protects data sent between your website server and a visitor's browser. HTTPS is becoming more and more necessary for all pages on a website, with some browsers such as Google Chrome marking pages without HTTPS as insecure.

To get HTTPS on all of your pages you will need an SSL certificate: Akamai supports shared SSL certificates or custom SSL certificates at a cost. section.io includes a unique SSL certificate for every account for no additional cost, and will manage the certificate for you so it never expires and puts your website at risk.

You should also consider the network protection offered: section.io is built on top tier cloud hosting, so you'll get all the DDoS network layer protection and capacity provided by industry heavyweights like Microsoft and Amazon. Akamai also provides significant protection against network-layer DDoS attacks due to their vast server network of servers.

Advanced Security Features

Both section.io and Akamai offer additional protection with features that detect and block malicious traffic. Akamai offers a Web Application Firewall and Bot Manager, while section.io provides a choice of Web Application Firewalls and is shortly releasing an advanced Bot Blocking tool.

Web Application Firewalls detect and block traffic from bad bots and hackers who may be trying to attack your website. They are able to patch known vulnerabilities and advanced WAFs can also find and patch unknown vulnerabilities.

However, not all WAFs are created equal: some are tricky to set up and may result in a high number of false positives, turning away legitimate traffic from your site and impacting potential revenue.

Akamai does not disclose the software behind their WAF although it is likely to be a modified version of the open-source software ModSecurity. section.io offers an unmodified version of ModSecurity, and Threat X , which is a next-generation intelligent WAF.

ModSecurity and Threat X both aim to protect your website from hackers and malicious bots, however they go about this in very different ways. ModSecurity uses rules that you set yourself to block traffic.

First, developers run ModSecurity in “Detect” mode to see what type of threats they are getting, and then they need to write rules to determine which threats need to be blocked. ModSecurity is a traditional binary WAF in which rules need to be turned on and off to block traffic without impacting legitimate traffic, and requires a significant amount of time from development teams to monitor and manage.

Threat X is an intelligent WAF that detects and blocks threats with no configuration needed from you. Threat X first runs in detect mode to learn your site’s legitimate traffic profile and threat profile, and then is switched to blocking mode where it automatically blocks threats without false positives that harm legitimate traffic

Threat X is different from other WAFs in that it identifies not only the entity performing the attack but also the level of progress made by the attacker by tracking threats across seven stages of attack and providing you with multiple response options.

Threat X is also backed by a team of security experts who monitor the latest hacker trends and how your website is being targeted, meaning you don’t need an advanced in-house security team to set up and manage their intelligent Web Application Firewall.

Akamai also offers bot blocking, which is included in section.io’s Threat X offering. section.io will also be releasing a smart bot blocking proxy in Q1 2017.

Continuous Integration and Continuous Delivery Support

Continuous Delivery and Continuous Integration are modern, agile development practices that require teams to regularly integrate code and deliver that code to production or a testing environment. By integrating and pushing changes regularly, companies get feedback more quickly and development teams reduce the risk that they have conflicts in their code.

Because small changes are released quickly, errors can be more easily identified and developers don’t need to search through a large code change to find issues.

CDNs including Akamai make it impossible for developers to follow a Continuous Integration or Delivery process because advanced configuration changes need to go through Akamai, purging code is not instantaneous, and there is no way for developers to test changes locally.

In addition, because Akamai and other CDNs use modified versions of reverse proxies, knowing how those modifications will impact code is very difficult.

section.io supports Continuous Integration and Delivery by giving users unmodified proxies that can be directly configured in the section.io portal. section.io also allows instantaneous purges and cache clears and real-time logs and metrics so teams can assess the impact of their code on metrics including cache hit rate.

Importantly, section.io is the only Content Delivery solution that provides a local development environment, so developers can test all changes locally before pushing to production.

This enables a process in which development teams are able to easily control and deploy configuration changes without the fear that issues will arise in production.

Pricing and Support

Pricing is an important component of any Content Delivery solution: you want a price that is transparent and easy to understand. Developers should be able to make changes themselves without engaging additional paid services which can vary widely in cost. If support is still needed, it should be a as a one-time training that enables developers to make future changes themselves.

Akamai pricing is not publicly released but can be based on pageviews, throughput, or Gigabytes and can include additional charges for extra features, Professional Services engagements, and SSL certificates. Because advanced configuration changes need to go through Akamai's Professional Services team, charges can quickly balloon.

section.io offers transparent pricing based on page views that includes SSL certificates, DNS hosting if neeeded, and other core features. The Plus plan includes fully configurable Varnish Cache for $149.95/month for 1,000,000 page views, plus unlimited additional page views at $0.25/1,000 pages.

The Max plan includes Varnish Cache plus a Web Application Firewall for $499.95/month for 1,500,000 pageviews plus unlimited additional page views at $0.45/1,000 pages.

The Threat X intelligent WAF can be added for an additional $599/month, and future reverse proxies can also be added for additional fees.

section.io's pricing is monthly and does not require any commitment. In addition, section.io allows websites to change or remove the reverse proxies they use at any time, so you are never locked in to specific tools. section.io regularly adds both open-source and proprietary reverse proxies, so users are always able to take advantage of the most advanced, modern technologies available on the market.

Conclusion

section.io and Akamai are both Content Delivery solutions with global server networks that aim to deliver improved speed, scalability, and security to their users. However, the two go about these improvements in very different ways which can have an impact on development team effectiveness, cost, and the performance and security improvements that are actually achievable.

Akamai was founded in 1998 and was the first Content Delivery Network at a time when slow connection speeds and an increase in Internet users were throttling and slowing down websites. Akamai remains the largest CDN with the highest number of global PoPs. However, for all but the largest global websites this high number of PoPs is unnecessary, and can actually have a detrimental effect on performance due to a lower cache hit rate.

Akamai has not adapted to agile, continuous development practices and makes it difficult for development teams to drive configuration changes themselves.

This results in a system which excels at basic static image caching but does not support dynamic caching. In addition, advanced configuration options need to be run through the Akamai Professional Services team which adds significant cost and time.

Akamai includes advanced security features such as a WAF and Bot Blocking. The Akamai WAF requires significant developer time to monitor traffic and write rules, and again advanced configuration changes may require Professional Services.

Overall, Akamai is a good solution for you if you are looking for a large, legacy CDN with a high number of PoPs and don't mind the integration challenges or cost implications that may come with those features.

By contrast, section.io has only 24 "Super PoPs" which are strategically placed along the internet backbone. section.io is a modern Content Delivery Grid which allows developers to control their configuration options, choose the proxies that work for them, and test changes locally before pushing to production.

section.io was born out of a frustration with legacy CDNs and the way they fail to integrate with agile development practices and make it difficult for developers to cache dynamic content and take advantage of other newer practices.

section.io aims to teach developers how to drive their own Content Delivery solution without needing to engage support or Professional Services: section.io offers enablement training when new teams sign on, which gives them the knowledge they need to achieve the best performance and security outcomes available.

The security offerings from section.io also embrace more modern philosopies, as Threat X's intelligent WAF is able to smartly detect and block threats while protecting legitimate traffic. section.io plans to add additional reverse proxies including smart Bot Blocking and Front End Optimization in 2017, and doesn't lock users into specific proxies or long term contracts.

section.io is ideal for companies who embrace modern development practices, don't want to pay for additional configurations, and want a choice of the best-in-class reverse proxies for performance and security.

GET IN TOUCH

section.io is the only website performance, scalability and security solution which gives developers complete, code-level control over reverse proxy configuration, testing, and global deployment.

Unlike legacy CDNs, who lock reverse proxies such as Varnish Cache and ModSecurity in fixed networks, section.io's Content Delivery Grid provides a software-defined content delivery solution so developers can easily customize their web performance and security composition.

To speak with a section.io representative or see a demo of the section.io platform please contact **sales@section.io** or visit **section.io/contact-us**.

If you'd like to get started yourself, visit **section.io/sign-up**.