section.io

Comparison Sheet: section.io and Cloudflare

A popular choice for small websites and blogs, Cloudflare provides basic performance and security benefits. However, its limitations, especially on the lower tier plans, can frustrate developers and make achieving the best outcomes for websites difficult. By contrast, section.io gives developers the tools they need to achieve the highest levels of both performance and security, including best-in-breed reverse proxies that are fully configurable. While Cloudflare provides small wins at a low cost, section.io is a holistic solution that gives websites maximum value as a Content Delivery solution and the ability to achieve the best possible performance, scalability, and security.

Feature	section.io	Cloudflare
Global delivery network	28 Super PoPs. More being released.	102 Super PoPs.
Caching/Performance	Static, dynamic and HTML doc caching	Static caching. Limited dynamic caching.
Security	Choice of Traditional or Intelligent WAF. DDoS protection and IP blocking.	Traditional rules-based WAF. DDoS protection and IP blocking.
Availability under peak traffic	High due to flexible caching config. Overflow Prevention feature can limit number of visitors on site concurrently.	Limited due to lack of HTML doc caching.
Reverse proxy choice	Choice of WAFs, current versions of Varnish Cache, plus Google's PageSpeed, OpenResty, Nginx, and more in future.	No choice of reverse proxies, versions of Nginx for caching and ModSecurity WAF.
Configuration options	Full software level control over configuration provided in portal with git backed workflow. No configuration limits.	Basic. Additional Page Rules must be purchased for caching config, WAF has just 25 custom rules up to Enterprise level.
Metrics & Diagnostics	Unlimited timespan metric access in portal or open end point querying. Real-time enriched logs available in	Very limited. Log access only at Enterprise level.
Development Integration	Full, software backed application development cycle integration.	Not offered.
Pricing	Caching Proxy: $149.95/month for 1,000,000 page views plus unlimited additional page views at $0.25/1000. Multiple Proxies: $499.95/month for 1,500,000 page views plus unlimited additional page views at $0.45/1000. Includes dedicated SSL certs, DNS hosting, HTTP/2, support, and full configuration of caching and security.	Monthly pricing starting with free plans for personal sites with limited support. Business plan at $200/month includes 25 custom WAF rules. Enterprise pricing for more advanced security, caching and logs is undisclosed, starts at several thousand dollars/month. Shared SSL and DNS hosting included.

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, availability, security, or a combination.

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 Cloudflare 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. Below we go through the core differentials between section.io, a flexible Content Delivery Grid with an intelligent WAF that is built to integrate with modern development processes, and Cloudflare, a traditional static-object caching Content Delivery Network with rules-based security offerings.

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. The DNS layer directs traffic to a network of servers or Points of Presence: Cloudflare and section.io both have networks of modern "Super PoPs" or Points of Presence around the globe. Cloudflare currently has 102 PoPs, and section.io has 28 PoPs.

Cloudflare is run on a global Anycast Network, which means that multiple machines can run the same IP address, and when a request is sent to an Anycast IP address it will be routed to the server closest to them.

section.io runs its hosted DNS system through an Anycast Network, and will be moving its Content Delivery Grid for HTTP requests to an Anycast Network in 2017.

While Cloudflare and section.io's networks are quite similar, it is important to note that the performance benefits seen by flexible caching considerations are considerably larger than those achieved by having a larger PoP footprint, as we explain in the next section.

Website Performance

The CDN reverse proxy layer 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.

Caching Reverse Proxy

section.io and Cloudflare both run caching reverse proxies as part of their Content Delivery solution. section.io offers a choice of unmodified Varnish Cache versions, while Cloudflare uses a modified version of Nginx.

Both Varnish Cache and Nginx can easily cache static objects such as images and documents. 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.

Caching Configuration

section.io and Cloudflare 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. section.io's platform allows for flexibility in what is cached and gives developers the control they need to cache all types of content.

Cloudflare uses a modified version of the Nginx caching proxy within their CDN. By default, Cloudflare caches only static content and does not cache HTML documents or other dynamic content.

Cloudflare users can set up Page Rules to cache more content, however these can be difficult to navigate and are limited in what they will do: Only one Page Rule will take effect on any given request, and Page Rules are given priority in an order from top to bottom. Because the reverse proxy is not open-source, troubleshooting when issues arise can also be difficult.

For applications who manage multiple domains, section.io makes it simple for all domains to be managed with one configuration and one account. Cloudflare requires users to set up separate accounts for each domain.

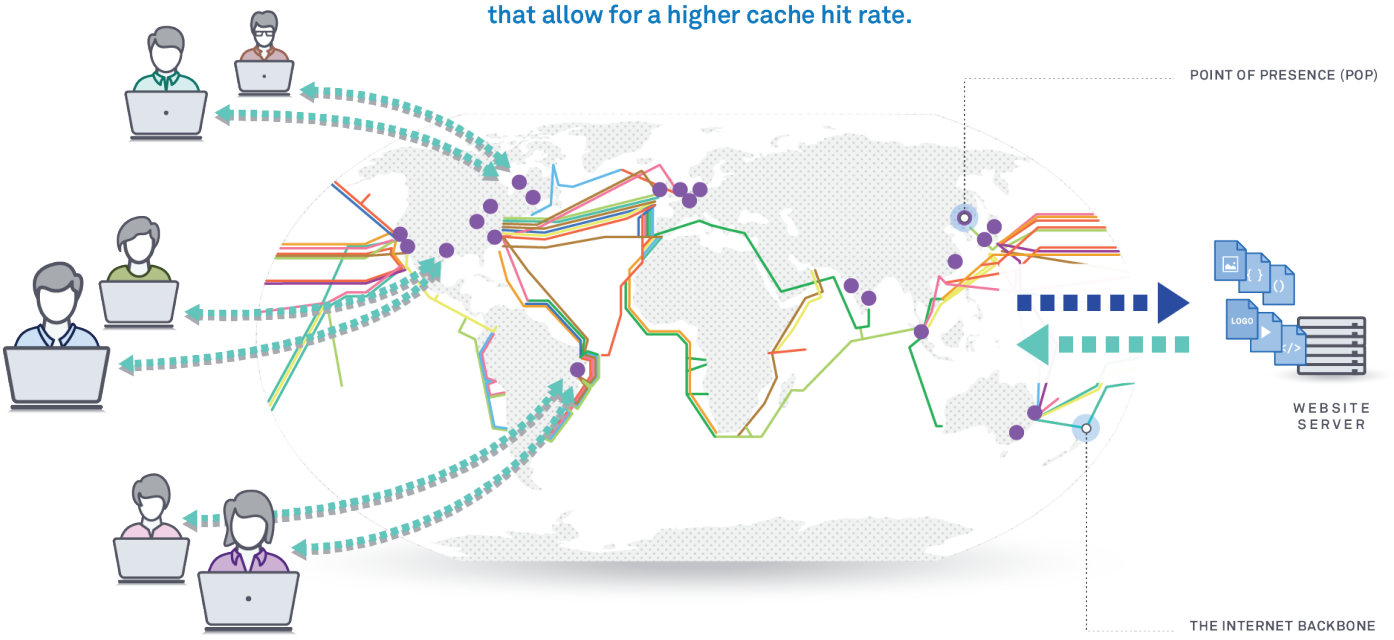
section.io's flexible configuration also enables different reverse proxies to be used for different sections of a website: www.shop.com could point to Magento and have caching and a WAF enabled, while www.shop.com/blog could point to Wordpress and have only caching enabled.

Search Engine Optimization

Cloudflare and section.io both provide additional performance benefits by serving all HTTPS traffic over HTTP/2, the updated and faster version of the HTTP communications protocol. Having HTTPS and HTTP/2 is also beneficial for SEO.

section.io gives websites the ability to re-write URLs for further SEO benefits, so blog.shop.com could be re-written to shop.com/blog, which is preferable for SEO.

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



Website Security

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: both Cloudflare and section.io provide SSL certificates at no extra cost, however Cloudflare's free certificates are shared among multiple websites, whereas section.io provides all users with a dedicated SSL certificate or the option to upload their own certificate at no extra cost. section.io also supports multiple SSL certificates for multiple domains running on the same section.io application.

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. Cloudflare also provides protection against network-layer DDoS attacks for even its free account tier.

Advanced Security Features

Both section.io and Cloudflare offer additional protection with features that detect and block malicious traffic. Cloudflare offers a Web Application Firewall with its Pro, Business, and Enterprise plans, while section.io offers a choice of Web Application Firewalls as part of its Max plan. section.io is also 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.

Cloudflare uses a modified version of the open-source software ModSecurity. section.io offers both 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. Threat X first runs in detect mode to learn your site's traffic profile and threat profile, and then is switched to blocking mode where it automatically blocks threats without false positives.

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.

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.

CDNs including Cloudflare make it impossible for developers to follow a Continuous Integration or Delivery process because advanced configuration changes are difficult and there is no way for developers to test changes locally. In addition, because Cloudflare uses 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.

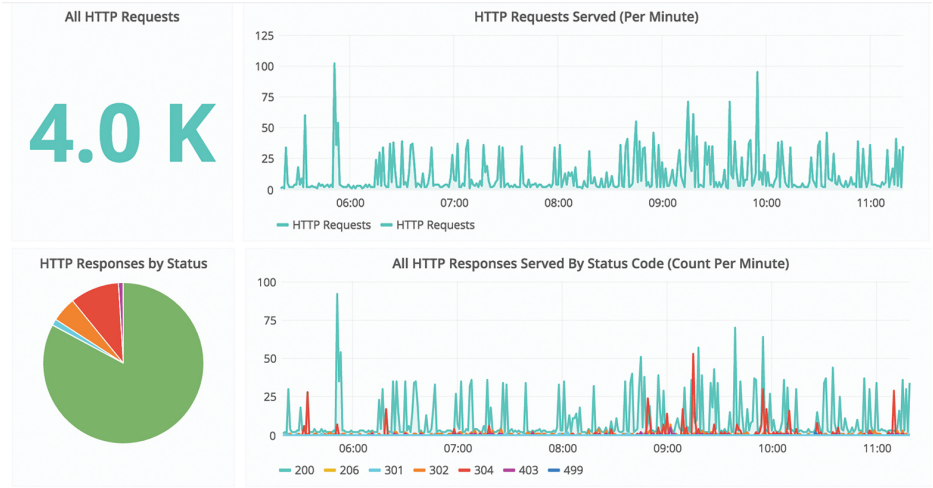
Importantly, section.io is the only Content Delivery solution that provides a local development environment, so developers can test all changes locally. This enables a process in which development teams are able to control and deploy configuration changes without the fear that issues will arise in production.

Metrics and Logs

Detailed logs and metrics that help identify and troubleshoot issues are an important part of any development cycle. section.io leverages the power of ElasticSearch and Kibana to provide request/response logs at a granular level. Easily filter requests based on status code, cache hit status, originating IP address and more.

section.io also provides in depth metrics that give you an aggregated view of how your CDN is performing. This includes website throughput and key proxy metrics, response count, error code rates, bandwidth, Varnish metrics by content type, and ModSecurity intercepts and passes. Threat X also provides a detailed dashboard with information on tracked and intercepted threats.

Cloudflare provides basic metrics including bandwidth saved, threats mitigated, website requests, and operational metrics. For logs of all requests that pass through the Cloudflare network accounts must be on the Enterprise plan.



Pricing and Support

section.io offers transparent pricing based on page views that includes SSL certificates, DNS hosting, and core features. The Plus plan includes fully configurable Varnish Cache, real-time logs and metrics, and core security features 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 page views 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 into specific tools.

section.io includes support through a live chat system, support tickets, and 24/7 support for the Max plan. If you are experiencing a business critical issue, section.io will always aim to respond as quickly as possible and assist you.

Cloudflare pricing varies from free to very high for Enterprise services. The Cloudflare free plan includes basic static image caching. The Pro plan at $20 per month includes static caching plus a basic, rules-based WAF. The Business Plan at $200/month includes a more advanced WAF and additional included Page Rules.

For sophisticated security with custom WAF rules, advanced DDoS support, header rewrites, edge side codes, and to have access to logs and metrics needed for troubleshooting, businesses must be on an Enterprise Cloudflare plan. Pricing for these plans is not released but starts at several thousand dollars per month.

Cloudflare offers email-only support for all plans except the Enterprise level. Response times range from a median of 13 hours for free plans to 25 minutes for Business plans. Those on the Enterprise plan have access to email and phone support with a 24/7 emergency-only hot line.

Conclusion

section.io and Cloudflare are both Content Delivery solutions 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.

Overall, Cloudflare is a good solution for smaller websites looking for basic caching and security. If you have a sophisticated internal development team or are looking to protect yourself from advanced attacks, Cloudflare's restrictions in advanced configurations and limited log access will limit what your team can achieve.

By contrast, section.io is built to be fully configurable and flexible, so that developers can cache both static and dynamic content and HTML documents. section.io provides developers with software-defined control over reverse proxy configuration, and gives them a local environment.

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

The security offerings from section.io also embrace more modern philosophies, as Threat X's intelligent WAF is able to smartly detect and block threats while protecting legitimate traffic. section.io is ideal for companies who embrace modern development practices, don't want to pay for additional configurations, and want to future-proof themselves with a choice of the best-in-class reverse proxies.

GET IN TOUCH

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**.