CLOUDFLARE®

Don’t Get Left Behind

Improving Your E-Commerce Site Performance and Security for the Mobile Consumer

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com

Executive Summary

Mobile is at the tipping point to become the most important channel of e-commerce strategies. The top 25% of U.S. retailers have already figured out how to drive up mobile conversion rates to take an overproportional share of the addressable market, in a race where the winners take it all. They manage to better retain users and attract product views by providing mobile sites and apps, which are fast and available. Cloudflare can help to achieve those critical requirements by providing:

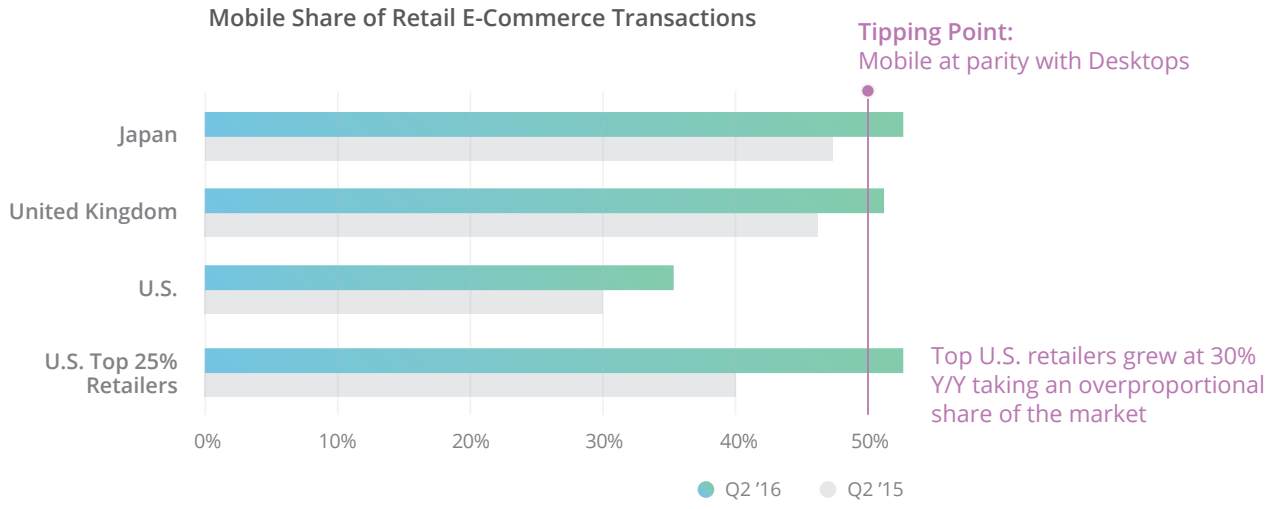
- One of the fastest Content Delivery Networks, based on Anycast routing and the ability to cache content physically close to consumers to reduce latency
- Predictable flat rate pricing
- Mobile Image and code optimization as well as support for IPv6 to reduce latency for mobile devices
- Protection against layer 3, 4 and 7 DDOS attacks and layer 7 application vulnerabilities to increase uptime
- Encryption done right with high performance

Setting up Cloudflare to get access to those capabilities is a major step forward for e-commerce vendors to proactively keep their sites fast and safe all year round.

Mobile commerce is at a tipping point

E-commerce is exciting: With 14.6% Y/Y growth in 2015—and accounting for a whopping 36.2% of US retail sales growth in 2015—it far outpaced brick and mortar retail growth. What is even more exciting is mobile commerce, which is growing even faster. Mobile commerce is now at a tipping point: For the first time ever, in Q2'16 in Japan and in the UK, the share of mobile e-commerce retail transactions was over 50% and thus larger than desktop transactions. In the U.S. the mobile share of e-commerce transactions is growing fast at 17% Y/Y. Even though the U.S. mobile share of e-commerce transactions is still trailing behind at 35% is it poised to catch up to the leading countries.

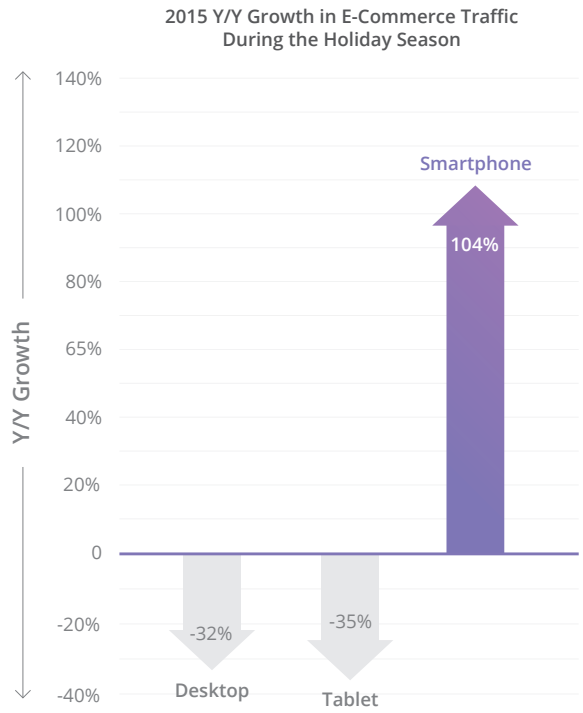
The leading quartile of US retailers are already capitalizing on this trend by providing the best mobile sites and apps. They manage to better retain users and attract product views, driving up their conversion rates by up to 90% compared to the average emerging retailer. As a result they are taking an overproportional share of the mobile spoil with 52% of their e-commerce sales coming from mobile, growing at a breathtaking 30% Y/Y.

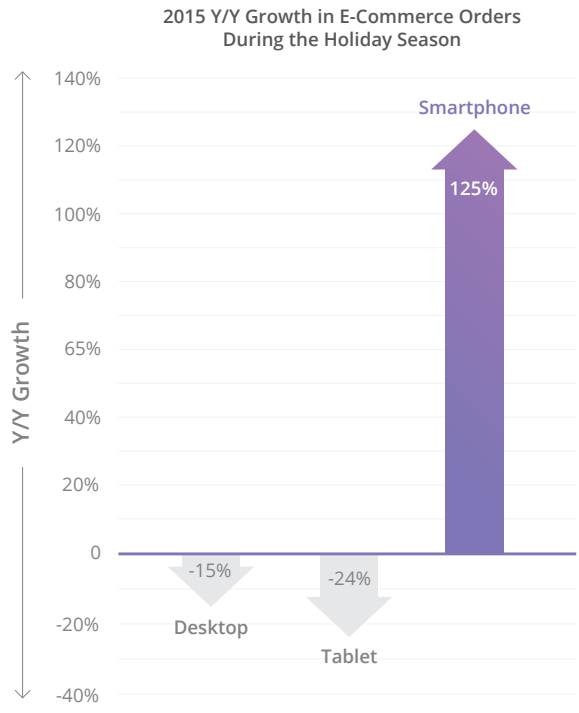


There can be no doubt that mobile commerce has developed into a key sales and marketing channel. The retailers providing the best mobile experience are the winners and will continue to take an even more dominant share of the available market.

Mobile is critically important for the holiday shopping season

Holiday online shopping (Cyber 5) broke records in 2015, with Cyber Monday claiming the title of the heaviest online spending day in U.S. history. Smartphones played a massively important role, claiming 49% of the traffic and 27% of the orders. Smartphone traffic and orders grew at amazing rates, on the cost of desktop and tablet traffic/orders, which shrunk accordingly.

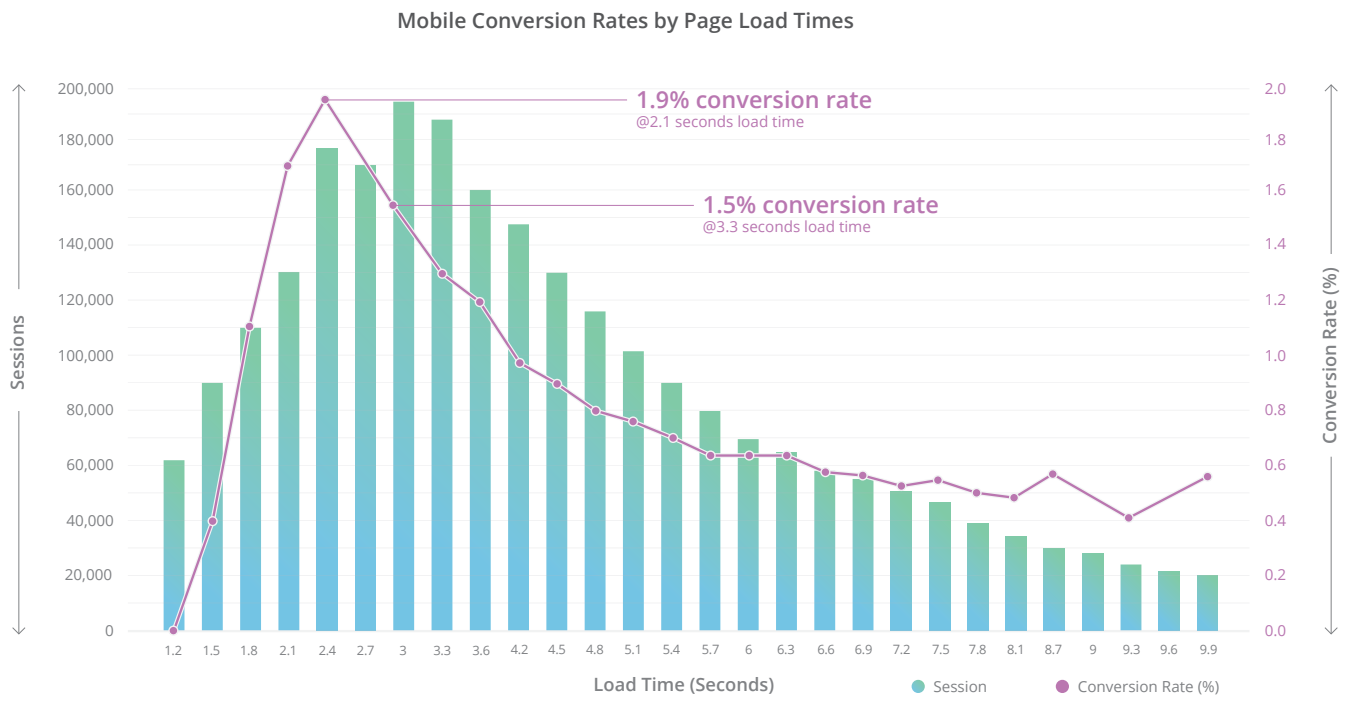




The Cyber 5 2015 shopping period proves again that the retailers with the best mobile experience clean the plate. For example, Amazon grew at 24.1% for the 2015 over 2014 Cyber 5 period. In the upcoming holiday season Brick and Click retailers will likely see more online than in-store traffic, making the mobile shopping experience critical for growth.

The impact of latency and availability on conversion rates

What separates the leaders from the pack? The leading e-commerce retailers provide the best mobile sites and apps to increase their conversion rates. Conversion rates for mobile are still low and they are directly linked to mobile site/app performance and availability. For example, the conversion rate for a leading online retailer peaked at 1.9% with an average page load time of 2.4 seconds. Only a one second slower average page load time of 3.3 second led to a drop of the conversion rate by 27%.

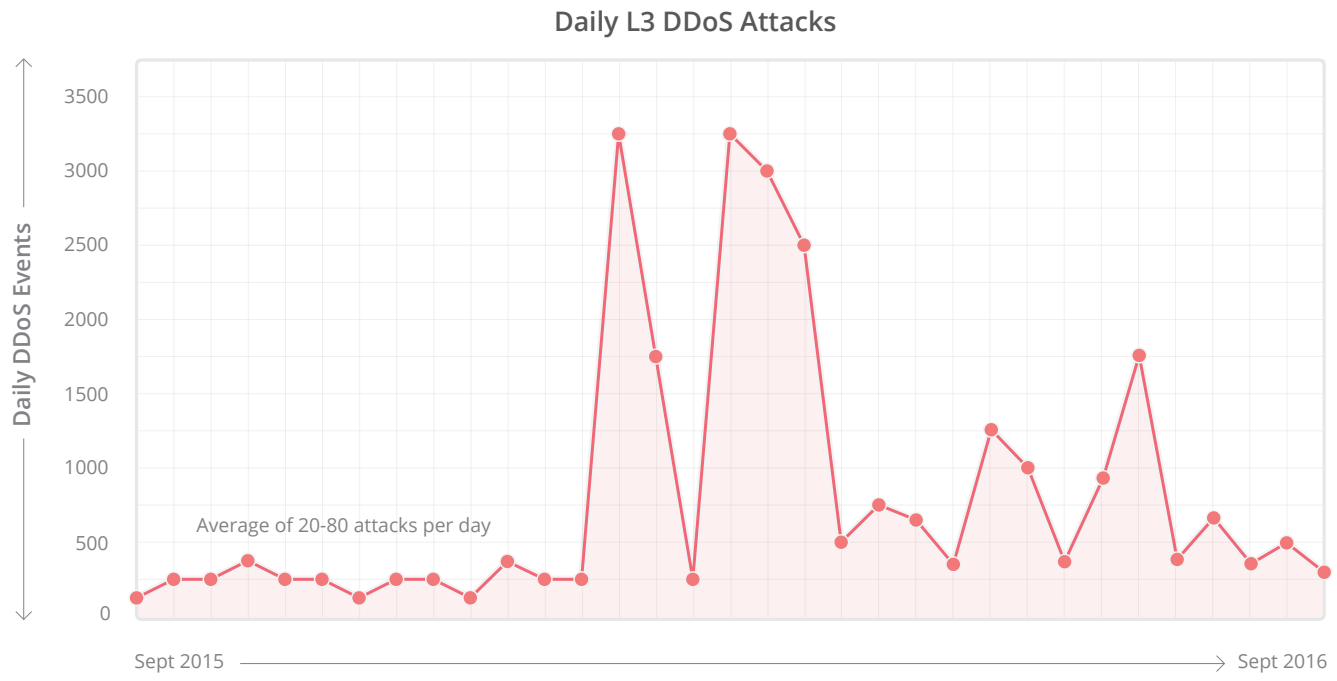


There are many industry examples, which illustrate the link between site performance and conversion rate

- Amazon increased revenue by 1% for every 100ms reduction in site latency
- Yahoo increased traffic by 9% for every 400ms reduction in site latency
- Walmart saw a sharp decline in conversion rates as average site load time increased from 1 to 4 seconds

In general, Google reported that site latency of 100 to 400 milliseconds has a measureable impact on consumer behaviour and a site, which is slower by 250 milliseconds than a competitor's site, will be less often visited.

In addition to latency caused by the sites/apps itself, Distributed Denial-of-Service (DDOS) attacks can make the site entirely unavailable. Cloudflare, which has close to 10% of the worldwide internet traffic flowing through its networks, can filter and accurately measure attacks. Over the last year Cloudflare saw the number and intensity of attacks increasing, with up to 1,400 DDOS events per day, an aggregated 400Gbps of incoming traffic and attacks with 200M packets per second.



Attacks are often not one off events and victims are typically targeted multiple times in a year. According to Cloudflare's experience anybody—large and small organizations—can be targeted. Even though many jurisdictions have laws under which DDOS attacks are illegal, there are DDOS-as-a-Service providers offering subscriptions, some starting as low as at $5 - $10/month.

Even Amazon's website ($99 Billion in retail revenues in 2015) went down multiple times in the past for unknown reasons. For example, in 2013 Amazon.com went down for an estimated 15-45 minutes, costing the company $1.8 - $5.3 million in lost sales, based on the company's average sales of $117,882 per minute. The cost of downtime to e-commerce vendors might be much higher during the holiday season—Amazon recognized 33% of annual revenues during the fourth quarter of 2015—due to the seasonality of the business. Other negative effects of system downtime include impact to customer satisfaction, search engine rankings and investor relations.

In summary, it is critical for e-commerce vendors, who want to improve conversion rates, especially during the holiday season, to provide snappy sites/apps, which are protected against DDOS attacks to improve uptime.

Essential technologies for fast and secure mobile sites

Cloudflare can help you to accelerate and protect your mobile commerce sites and apps, without adding hardware, installing software, or changing a single line of your code.

The first step is to use Cloudflare's Content Delivery Network (CDN), which is one of the world's largest networks that powers more than 10 trillion requests per months. This is nearly 10 percent of all internet requests for more than 2.5 billion people worldwide. Cloudflare's CDN is consistently ranked as one of the fastest CDNs with median response times of 34 ms (for the US) according to Cedexis. Some of its key capabilities include:

Anycast based routing

While Cloudflare's CDN works with a routing scheme called Anycast, most of the internet today still works with a mechanism called Unicast. Under Unicast, every node on the network gets an IP address, which is unique to it. Routers keep a map of the world's IP addresses to maintain a sense of the shortest path across the various hops to reach the final destination. However, the final destination might be somewhere across the continent or in some other place around the world, requiring additional hops, which each add latency. Under Anycast, the routing scheme used by Cloudflare, multiple machines in the CDN network share the same IP address allowing routers to send requests directly to the physically closest server and to reduce latency.

Caching of content

Cloudflare's Anycast network operates in conjunction with caching of content. Once Anycast routed a request to the physically closest server, a copy of cached content is available for access on this server. The benefits of caching are that objects can be moved closer to the visitor requesting them to accelerate delivery, and to decrease the load on the origin web server. Cloudflare provides capabilities for automatic caching of static content, and with Railgun Cloudflare provides a mechanism to cache dynamic content.

Cloudflare analyzes the traffic that passes back through the servers in the CDN to find the static portions of the origin site. Then the static content is cached in the CDN for a short period of time. Typically 66% of web content is cacheable (through "automatic caching of static content") and the remaining 34% is non-cacheable and must be obtained from the origin web server. Railgun is designed to speed up the delivery of content that cannot be cached so that essentially the entire web becomes cacheable. It works by recognizing that uncacheable web pages do not change very rapidly and the very small difference in changes between versions of the web pages can be identified by Cloudflare's CDN servers. Cloudflare then compresses the changes with compression rates of up to 99.6% and sends them across the link, achieving performance improvements of up to 700%. Railgun requires the installation of a software component on the origin server side.

"As bandwidth costs continue to rise having a CDN like Cloudflare serving images on the edge to users is both cost effective and reduces latency for our mobile customers"

Chris Smith, Director of E-Commerce, Big 5 Sporting Goods

Flat rate pricing

To be a part of the Internet, Cloudflare buys bandwidth, known as transit, from a number of different providers. Cloudflare buys transit wholesale on the basis of the capacity used in any given month, paying for maximum utilization for a period of time. While the rate Cloudflare pays varies dramatically from region to region around the world, to keep pricing simple, Cloudflare charges customers a flat rate regardless of where the traffic is delivered around the world. Unlike some cloud services, which bill for individual bits delivered across a network, Cloudflare makes monthly bills predictable. Cloudflare continues to work to decrease the transit pricing, and increasing peering, in order to offer the best possible service at the lowest possible price.

Image and code optimization

With Polish, Mirage and Auto-Minify Cloudflare provides a one-two-three punch to reduce latency. Those capabilities are especially important for mobile devices, which have limited bandwidths.

Polish removes metadata and compresses images to decrease their size. Polish can be run in Lossless mode, which removes the unnecessary bloat from the image header and metadata without removing any image data. The average file size is reduced by 21%. Polish can also be run in Lossy mode, which in addition to Lossless applies a compression algorithm to suitable images. Images will appear exactly the same as they would have before, without any perceptible visual difference, but the average file sizes are reduced by 48%. Images make up more than 50% of the data that makes up a typical website.

Mirage manages how images are loaded on mobile devices. It quickly produces the appearance of a usable page for users to interact with, while filling in the rest of the page without disrupting the user experience.

- Mirage uses Lazy Loading to prioritize the loading of the images that are in the viewport i.e. the images that are actually displayed by the browser. It then loads the other images on the page, which are not displayed by the browser, as they are needed or as there are spare network resources available.
- Mobile devices require smaller images due to their smaller screen size. Mirage resizes an image at the server to typically as little as 1% of the full-resolution image and sends the reduced-size image first. After the page is rendered with the reduced-sized images they will be replaced by the full-resolution versions. Images start to appear first as low quality and then come into sharp focus.
- Rather than initiating a new request for each image, Mirage streams all the images from Cloudflare's network with a single request.This means that even a page with hundreds of images can begin rendering in the browser with as few as two requests. Even users on slow mobile connections can begin interacting with the page immediately, rather than having to wait for all the full-resolution images to load

Auto Minify removes on-the-fly all unnecessary characters—i.e. the "whitespace"—from HTML, JavaScript and CSS files, saving 20% of a file's size without changing an of the functionality. Cloudflare implementation of Auto Minify is easily 100x faster than the next closest approach.

Support for IPv6

Real User Monitoring measurements by Facebook and Linkedin showed that mobile page load times over IPv6 are well over 10% faster than over IPv4 for the top-4 US mobile networks. While the roll-out of IPv6 is a multi-decade activity and is suffering from the perception of being slow, around 60% of Android and over 20% of iPhone requests from the top-4 US mobile networks used IPv6 on dual-stacked sites (as of 5/4/2016). Cloudflare has not only offered full IPv6 support as well as an IPv6-to-IPv4 gateway since 2012, Cloudflare also makes it "one click simple" for customers to enable this service. If the origin server supports IPv6 then visitors arriving on an IPv6 connection will be transported via the protocol end-to-end. If the origin server only supports IPv4, Cloudflare will accept a visitor over IPv6 and then seamlessly make a request to the server over IPv4. In addition, if an application running on the origin server has a hard requirement to run on IPv4, Cloudflare provides Pseudo IPv4. This option will, whenever a connection is established over IPv6, add a HTTP header to requests with a "pseudo" IPv4 address.

Layer 3 and layer 4 DDOS protection—Anycast network resilience with automatic learning platform

In addition to using Cloudflare's Content Delivery Network (CDN) the next step is to protect the site/apps against malicious attacks to ensure uptime. Cloudflare's advanced DDoS protection, provisioned as a service at the network edge, matches the sophistication and scale of the threats and can be used to mitigate DDoS attacks of all forms and sizes. Cloudflare prevented multiple of the largest DDOS attacks including attacks with more than 400Gbps.

Layer 3 and layer 4 DDOS attacks are usually volumetric attacks such as DDOS amplification, DDOS flood and DDOS SYN flood attacks. While those attacks can overwhelm a typical unicast based network, Cloudflare's Anycast based network inherently increases the surface by spreading the attack traffic to each of the more than 100 Cloudflare datacenters and to a diverse set of high bandwidth interconnections with other networks, to simply absorb the attack traffic. In addition Cloudflare provides an automatic learning platform, where network traffic is analyzed in real time to identify anomalous or malicious requests. Once a new attack is identified, Cloudflare automatically starts to block that attack type for both the particular website and the entire community.

Even from a cost perspective, attacks usually don't impact Cloudflare: Cloudflare buys significant amount of wholesale bandwidth and pays for the higher of the ingress (inbound) or egress (outbound) traffic averaged over a month. Since Cloudflare acts as a caching proxy, under normal circumstances egress always exceeds ingress, usually by around 4-5x. When there's an attack, the two lines get closer together but rarely is an attack large enough to add to Cloudflare's overall bandwidth costs. Cloudflare passes on this benefit to their customers and customers are not being charged for an increase in network traffic caused by a DDOS attack.

As Cloudflare continues to grow its network and its community, it will get harder and harder to launch an effective DDoS attack against any of Cloudflare's users.

Layer 7 DDOS protection—Rate Limiter with IP Reputation Database

Like Layer 3 and 4 volumetric attacks, Layer 7 Denial of Service attacks use a high volume of requests to prevent real users from accessing a website. In layer 7 Denial of Service attacks a single IP address makes many requests, which are similar to the pattern of normal non-malicious traffic, and thus they are difficult to protect against.

Cloudflare's Traffic Protector—currently available through an Early Access Program—tracks the number of requests coming to a site from each IP address and identifies sites, which are making too many requests per minute. Once a suspicious IP address is identified, traffic from this IP address is presented with an interstitial page for about 5 seconds to perform a series of mathematical challenges. If the request fails this challenge, Traffic Protector downgrades that IP's reputation and traffic from this address will be shown a CAPTCHA page with every access attempt.

When Cloudflare identifies an IP addresses that appears to be making malicious requests it is stored in the Cloudflare IP Reputation Database. Based on a threat score a request either goes through or the request is presented with a CAPTCHA. If the CAPTCHA fails and the IP address is identified as malicious, the request is blocked at Cloudflare's edge for the entire network, benefiting the entire Cloudflare community.

Layer 7 non-DDOS application vulnerability attacks—Web Application Firewall

Layer 7 application layer attacks are the most complicated and sophisticated types of attacks. By mimicking normal use of an application, they are able to get past most DDoS mitigation equipment and vulnerability protection services. Common types of attack include SQL injection and Cross-Site Scripting (XSS), which might allow attackers to access and temper with customer or any other kind of application data.

Cloudflare addresses those threats via its Web Application Firewall (WAF). The WAF implements the OWASP Core Rule Set, Cloudflare provided out of box rules, as well as custom rules created by the community/customers. A new rule released by Cloudflare will propagate to all Cloudflare server nodes within 30 seconds and the WAF itself adds less than 1ms of latency per request, providing security without any performance tax. This way Cloudflare has been able to protect their customers against major Zero-Day vulnerabilities including the Shellshock vulnerability or the Heartbleed Bug.

> "We take the impact of a DDOS attacks very seriously. Even in those instances when our domain has faced a DDOS attack, Cloudflare was able to protect our domain quickly, providing a seamless experience for our customers. The single biggest benefit Cloudflare provides to us is peace of mind that someone is monitoring the network and that you have a way to mitigate any attack"
>
> Chris Smith, Director of E-Commerce, Big 5 Sporting Goods

TLS 1.3 and HTTP/2 with Server Push

Encryption is essential to provide a trustworthy shopping experience, but the latest SSL enhancements can be used to do it right and increase performance. Transport Layer Security 1.3 (TLS) not only removes insecure features of previous TLS versions, it also reduces latency by cutting the round-trip of the protocol in half. Cloudflare was first to deploy TLS 1.3 and heavily contributed to the standard. Cloudflare was also first to deploy HTTP/2, which only works with TLS. HTTP/2 increases performance, especially latency, as perceived by the end-user while using a browser. HTTP/2 works in combination with Server Push, where a server can send resources the client has not yet requested to accelerate perceived performance even more. TLS 1.3 and HTTP/2 with Server Push are just two examples of Cloudflare's effort to constantly integrate emerging technologies into its network.

Takeaways

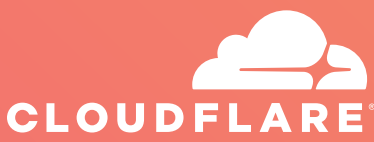
Sign up with Cloudflare to improve the performance of your mobile site and apps while protecting them from DDOS attacks and application vulnerabilities. The set up is easy and usually takes less than 5 minute to get up and running. Check out the plans, ranging from free to enterprise at www.cloudflare.com.

To learn more about Cloudflare, please contact us.

www.cloudflare.com

enterprise@cloudflare.com

1 888 99 FLARE



1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com