CLOUDFLARE®

A Network for Blazing Fast and Secure Content Experiences

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

I. Executive Summary

As user expectations for speed, stream quality, and image quality grow, performance becomes more and more crucial for growing media and entertainment companies. At the same time, companies must balance these demands with the need to keep their data, and their customers' data, secure.

In this white paper, we will go over why security and performance matter to your business, the threats faced by media and entertainment platforms today, the factors that impact performance, and how you can improve your security posture while simultaneously boosting performance.

II. Why are performance and security important for media and entertainment platforms?

Performance

Web performance affects the overall user experience of any media and entertainment business. Websites and applications need to load fast and respond to user actions quickly in order to keep users engaged and increase conversions.

Making matters more complex is the geographically distributed nature of today's audiences. Viewers and readers all around the world expect fast, high-quality experiences, regardless of device, connection type, or location.

Research shows that users are very willing to abandon applications, websites, and videos that are slow-loading or fail to load altogether:

- 39% of users stop engaging with a website if images take too long to load.[1]
- 85% of respondents stop watching video if it takes too long to load.[2]
- 30% of users are likely to stop watching a video if the stream is of poor quality.[3]
- Each 1-second buffering delay for video playback results in a 5.8% percent increase in abandonment rates.[4]

Expectations are even higher for live streaming content: 67% of viewers say quality is the most important factor when watching a live stream.

Finally, site speed also plays a crucial part in your SEO rankings. Google has included site speed as a factor in their search rankings since at least 2010.6 For websites that rely on organic traffic and high placement in search results (such as news websites), following good SEO practices is critical. This entails ensuring that all content loads as quickly as possible.

Security

Media and entertainment platforms increasingly must prioritize cyber security in order to remain online and functional. Cyber crime is on the rise, making an investment in cyber security a must for every organization. 61% of firms suffered a cyber attack from July 2018 to July 2019, up from 41% in the previous 12 months. [7] Media and entertainment companies are no exception to this trend.

A variety of threats can result in negative business outcomes. Data breaches undermine consumer confidence and can reveal compromising or confidential information to the public. Ransomware has immediate financial costs in addition to bringing normal business operations to a halt.

But media platforms particularly need to worry about attacks that impact their performance and reliability: **Denial-of-service (DoS)** and **distributed-denial-of-service (DDoS)** cyber attacks can disrupt normal services, impacting content load times, vastly slowing down video streaming, and crashing websites. Studies have shown that if content cannot load quickly, users will abandon the app or website: The BBC found that 10% more site visitors left for every additional second it took for their webpages to load.[8] Thus, DoS and DDoS attacks that slow down web performance can vastly cut down on total user traffic and engagement.

III. What factors affect performance?

For content providers and media and entertainment platforms, maintaining fast performance has become more of a challenge than ever.

The challenges of Streaming

Video files are much larger than almost every other file type available over the Internet. Because of this, video is streamed, not downloaded. In streaming, video files reach users a little bit at a time, and apps or browsers on the client side play the video files as they are received. This means that the file is continually sent to the user as they watch it, and an interruption in the stream causes the video to stop playing.

Streaming is subject to the same kinds of delays and performance degradations as other kinds of web content. Because the streamed content is not stored on the client device, hosting location makes a big difference for network latency. If a user in New York is trying to stream from a server in California, the video content will have to cross 3,000 miles in order to reach the user, and the video will have to spend a long time buffering or may not even play at all.

Dropped packets

All data that crosses from one point to another on the Internet is broken up into packets. These data packets travel based on transport protocols.

Streaming video and audio files traverse the web using a transport protocol called UDP. In contrast with the TCP protocol, which is used for most content on the Internet, UDP does not establish a connection before sending data packets, nor does it verify that all packets arrive. This makes streaming much more efficient, but if too many packets are dropped in transit, users will experience lower stream quality.

Network issues

Users access Internet properties from all kinds of networks, and network conditions play a huge role in how well your website or app performs.

Bandwidth measures the maximum amount of data that can pass through any given point on a network at once. A user's network may not always provide enough bandwidth for a quality web browsing experience. Limited bandwidth can especially impact the video streaming experience.

Network latency is partially caused by distance. The farther a user is physically from an origin server, the more latency there will be. The speed of light is a hard limit on how fast data can travel, and data will take from a few milliseconds up to nearly a second to travel from the user to the server and back.

The effects of network latency can be somewhat reduced by using a CDN — content delivery network — to cache content closer to users, and by deploying a global load balancer. Major content providers such as Netflix make extensive use of CDNs.[9]

Network congestion occurs when network traffic exceeds bandwidth at a certain point on the network, whether that's within an Internet Exchange Point (IXP), in a data center, or on a LAN router in a home. The resulting network congestion leads to slower Internet speeds for anyone connected to the network.

If multiple people are trying to stream high-definition video at the same time, within the same house for instance, this can cause network congestion. The same principle applies if more users are streaming video within a given region than the infrastructure is equipped to handle. This is another reason why content providers make extensive use of CDNs — to limit network chokepoints and network congestion by pushing content as close to users as possible.

IV. What cyber threats do media and entertainment platforms face?

DDoS attacks

DDoS attacks pose a significant risk for entertainment and media companies. DDoS attacks are especially a concern because they are growing in size and frequency. Attacks 100Gbps in size and higher increased by 967% between Q1 2019 and Q1 2018.[10] An attack detected in January 2019 set a record for most packets per second: 580 million.[11]

Major German media outlet Handelsblatt has faced regular DDoS attacks over the years.[12] In 2015, DDoS attacks knocked all BBC websites offline for an extended period of time.[13]

Shortly thereafter, many Irish government and news websites faced DDoS attacks.[14] More recently, Wikipedia was knocked offline in September 2019 by a massive DDoS attack.[15] The attack disrupted access to the website for several hours.

These events prompted some news outlets to look for better DDoS protection. Michael Kennedy, Technology Infrastructure Manager at Ireland's national public-service media organization RTÉ, explained:

> "We're the most trusted source for news and current affairs content. People rely on RTÉ. We needed to take measures to protect our services because we knew our current resources would not keep our sites online."[16]

Site hijacking

Any public-facing website with a high amount of visitor traffic makes a tempting target for attackers — attackers either with an agenda or just looking for amusement. Often, the result is website defacement, which is when the content on a website is altered by an external party. For instance, in 2013 the Vogue Magazine UK website was hacked to display irrelevant images.[17]

In such cases, attackers often gain access through exploiting vulnerabilities. Common website exploit attacks include cross-site scripting, SQL injection, and account takeovers, among others. The non-profit Open Web Application Security Project (OWASP) tracks web vulnerabilities, and their top 10 list of vulnerabilities is as follows:[18]

1. Injection (such as SQL injection)
2. Broken user authentication
3. Sensitive data exposure
4. XML external entities
5. Broken access control
6. Security misconfigurations
7. Cross-site scripting (XSS)
8. Insecure deserialization
9. Components (such as libraries or frameworks) with known vulnerabilities
10. Insufficient logging and monitoring

A web application firewall (WAF) can stop these kinds of attacks. Learn more about WAFs in Part V of this paper.

Content scraping and other bot attacks

A large percentage of Internet traffic comes from bots.[19] While some of these bots are harmless or even helpful, malicious bots can slow down website performance, steal content, put unnecessary strain on servers, and hijack user accounts.

Content scraping is of particular concern to media properties. The production of original content is what keeps consumers coming back. If competitors scrape content, media outlets lose their main advantage (at least temporarily). If malicious actors scrape content, they could use it to deceive users into visiting an unsafe website they control, undermining consumer trust.

In a content scraping attack, bots crawl and download all content on a website rapidly. This involves sending HTTP GET requests in rapid succession until the bot has obtained all the content it can find. Often the content is then reproduced elsewhere on the web. Because content scraping involves requesting content much faster than a real user is capable of, bot management products are usually capable of identifying content scraping attacks.

V. What steps can you take to improve performance and security?

Steps to improve performance:

1. Audit and optimize site images

The user's browser needs to download images before they can be displayed. The larger an image is (in terms of file size, not dimensions), the longer it takes to download. Large images often add to the load time of a webpage unnecessarily, as many devices don't have good enough screen resolution or a large enough screen to make very high resolution images necessary.

Before images can be optimized, you should determine how many images your website has and where they are located by conducting an image audit. Following the audit, as many images as possible should be optimized — meaning, compressed, resized, and converted to a lossy file format such as JPEG. Optimized images will load much more quickly.

Moz.com has step-by-step instructions for crawling all images on your website, identifying which ones need to be optimized, and optimizing them. Screaming Frog's SEO website crawler is helpful for auditing website images.

Cloudflare Image Resizing, Mirage, and Polish are the best options for companies that already deploy the Cloudflare CDN in order to cache images for faster delivery. Cloudflare Polish can be activated in the Speed tab of the Cloudflare Dashboard.

2. Use a CDN

CDNs are essential for any Internet property that has large media files. A CDN is a network of caching servers that cache and serve content so that requests and responses don't have to travel all the way to and from a web property's origin servers. CDNs move content closer to end users, vastly cutting down on latency. Additionally, by caching content in multiple locations, no one server or network gets overwhelmed with requests for content. Leading video content providers such as Netflix[9] and Hulu[21] make extensive use of CDNs.

3. Leverage a global and local load balancer

If origin servers are overloaded, they will perform slowly. Check the memory utilization of your servers. Are some machines working harder than others? Are some servers using all of their compute power while others aren't? To get the most performance out of your servers and utilize server resources efficiently, it's important to balance workloads across multiple servers.

Cloudflare Load Balancing provides local and global load balancing to reduce latency, either by load balancing traffic across multiple servers or by routing traffic to the closest region. It also includes health checks with fast failover to rapidly route visitors away from failures.

Load balancing is also important for complying with regulations such as the General Data Protection Regulation (GDPR). By routing traffic to the closest data center geographically, user data does not have to leave its region of origin, reducing the risk of being out of compliance.

Steps to improve security

1. Use a web application firewall (WAF)

WAFs sit in front of web properties, applications, and APIs in order to block malicious traffic, including vulnerability exploits and other types of cyber attacks. Gartner notes that "cloud-delivered WAF services [have] become the preferred choice to protect public-facing web apps."[22]

The Cloudflare WAF runs in the cloud and protects your web applications from malicious attacks with no changes to your existing infrastructure. Cloudflare is able to evaluate traffic to and from over 1 billion IPs and analyze digital signatures for potential threats and exploits, every day. The Cloudflare engineering team leverages Cloudflare's proprietary threat intelligence to update the WAF's rulesets regularly.

2. Turn on strong DDoS protection

Staying online and available in the face of DDoS attacks is a must for media and entertainment platforms. By rate limiting user sessions, filtering out known bots, and distributing requests to a CDN instead of sending all requests to the same servers, most DDoS attacks can be effectively neutralized.

The Cloudflare global network has enough capacity to mitigate DDoS attacks larger than the largest currently on record. Cloudflare provides unlimited and unmetered mitigation against sophisticated DDoS attacks at layers 3, 4, and 7 of the OSI model, all without blocking legitimate web traffic.

3. Protect against malicious bots

Bot management refers to blocking undesired or malicious Internet bot traffic while still allowing useful bots to access web properties. Bot management accomplishes this by detecting bot activity, discerning between desirable and undesirable bot behavior, and identifying the sources of the undesirable activity.

Cloudflare Bot Management is able to leverage the threat intelligence from billions of requests flowing through its network per day to identify good and bad bot traffic. You can manage good and bad bots in real time with speed and accuracy by harnessing the data from Cloudflare's more than 26 million Internet properties.

4. Closely track analytics

Without visibility into what is actually happening with your web properties, it is difficult to make effective decisions about security. From analyzing the types and origins of the web traffic you receive to tracking the health of your origin servers, real-time analytics are essential for understanding the performance and security challenges you are facing at any given time.

Cloudflare Analytics empowers you with deep insights and intelligence to protect and accelerate your Internet property. In addition to monitoring your servers and setting up failovers if necessary, you can create customized dashboards with all the data you need.

VI. Should you prioritize security or performance?

Often content providers find themselves having to choose between performance and security. Security is crucial, but cyber security solutions sometimes slow down normal processes, forcing companies to compromise performance for security.

However, Cloudflare offers a way for media and entertainment companies to boost performance and security simultaneously. All Cloudflare products run on the same global anycast network, which reduces latency because

traffic never has to be routed to distant scrubbing centers for security. Additionally, all Cloudflare products are tightly integrated in a single control plane. This enables you to accelerate the experience for your users while also protecting your users and your infrastructure.

Contact Cloudflare to learn more about solutions for entertainment and media: enterprise@cloudflare.com

About Cloudflare

Cloudflare, Inc. (www.cloudflare.com / @cloudflare) is on a mission to help build a better Internet. Cloudflare's platform protects and accelerates any Internet application online without adding hardware, installing software, or changing a line of code. Internet properties powered by Cloudflare have all web traffic routed through its intelligent global network, which gets smarter with every request. As a result, they see significant improvement in performance and a decrease in spam and other attacks. Cloudflare was named to Entrepreneur Magazine's Top Company Cultures 2018 list and ranked among the World's Most Innovative Companies by Fast Company in 2019. Headquartered in San Francisco, CA, Cloudflare has offices in Austin, TX, Champaign, IL, New York, NY, San Jose, CA, Seattle, WA, Washington, D.C., Lisbon, London, Munich, Beijing, Singapore, and Sydney.

Endnotes

1. “The State of Content: Expectations on the Rise.” Adobe, https://blogs.adobe.com/creative/files/2015/12/Adobe-State-of-Content-Report.pdf. Accessed 24 July 2019.

2. Dahl, Jon. “How do users feel about video streaming quality on their TVs?” Mux, https://mux.com/blog/how-do-users-feel-about-video-streaming-quality-on-their-tvs/. Accessed 9 August 2019. h/t https://www.emarketer.com/content/half-of-u-s-users-stop-viewing-content-slow-to-load

3. “Quality Matters: Video Streaming Quality Report 2016.” Verizon, https://www.verizondigitalmedia.com/report/quality-matters/. Accessed 9 August 2019. Gated. Secondary source: “’It’s Still Loading?!’ Long Load Time Just One Reason People Quit Watching Video.” eMarketer, https://www.emarketer.com/Article/Its-Still-Loading-Long-Load-Time-Just-One-Reason-People-Quit-Watching-Video/1015717. Accessed 9 August 2019.

4. Krishnan, S. Shunmuga and Ramesh K. Sitaraman. “Video Stream Quality Impacts Viewer Behavior: Inferring Causality Using Quasi-Experimental Designs.” IEEE, https://people.cs.umass.edu/~ramesh/Site/HOME_files/imc208-krishnan.pdf. Accessed 9 August 2019.

5. Golum, Caroline. “Live Video Statistics: What Consumers Want [Infographic].” Livestream, https://livestream.com/blog/live-video-statistics-livestream. Accessed 9 August 2019.

6. Singhal, Amit, and Matt Cutts. “Using site speed in web search ranking.” Google Webmaster Central Blog, https://webmasters.googleblog.com/2010/04/using-site-speed-in-web-search-ranking.html. Accessed 22 July 2019.

7. “Cybersecurity Firms See Increase in Cyber Attacks.” Security Magazine, https://www.securitymagazine.com/articles/90483-cybersecurity-firms-see-increase-in-cyber-attacks. Accessed 24 February 2020.

8. Clark, Matthew. “How the BBC builds websites that scale.” CreativeBloq, https://www.creativebloq.com/features/how-the-bbc-builds-websites-that-scale. Accessed 22 July 2019.

9. Macauley, Tom. “Ten years on: How Netflix completed a historic cloud migration with AWS.” Computerworld, https://www.computerworld.com/article/3427839/ten-years-on--how-netflix-completed-a-historic-cloud-migration-with-aws.html. Accessed 9 August 2019.

10. Rayome, Alison DeNisco. “Major DDoS attacks increased 967% this year,” TechRepublic, https://www.techrepublic.com/article/major-ddos-attacks-increased-967-this-year/. Accessed August 6, 2019.

11. Nohe, Patrick and Casey Crane. “The Largest DDoS Attacks in history.” Hashed Out, https://www.thesslstore.com/blog/largest-ddos-attack-in-history/. Accessed 24 February 2020.

12. “How Cloudflare is Powering Handelsblatt Media Group’s Digital Transformation.” Cloudflare, https://www.cloudflare.com/case-studies/handelsblatt-media-group-digital-transformation/. Accessed 24 February 2020.

13. “Web attack knocks BBC websites offline.” BBC, https://www.bbc.com/news/technology-35204915. Accessed 24 February 2020.

14. Leyden, John. “Irish government websites hit by widening DDoS attacks.” The Register, https://www.theregister.co.uk/2016/01/22/irish_gov_ddos/. Accessed 24 February 2020.

15. Butcher, Mike. “Wikipedia blames malicious DDoS attack after site goes down across Europe, Middle East.” TechCrunch, https://techcrunch.com/2019/09/07/wikipedia-blames-malicious-ddos-attack-after-site-goes-down-across-europe-middle-east/. Accessed 24 February 2020.

16. “RTE.” Cloudflare, https://www.cloudflare.com/case-studies/rte/. Accessed 24 February 2020.

17. “The 5 Funniest Hacked Website Defacements I’ve Ever Seen.” Blueshoon, https://www.blueshoon.com/the-5-funniest-hacked-website-defacements-ive-ever-seen/. Accessed 24 February 2020.

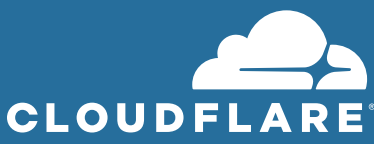
18. “OWASP Top Ten.” OWASP, https://owasp.org/www-project-top-ten/. Accessed 24 February 2020.

19. Hughes, Matthew. “Bots drove nearly 40% of internet traffic last year — and the naughty ones are getting smarter.” The Next Web, https://thenextweb.com/security/2019/04/17/bots-drove-nearly-40-of-internet-traffic-last-year-and-the-naughty-ones-are-getting-smarter/. Accessed 24 February 2020.

20. “2019 Data Breach Investigations Report: Executive Summary.” Verizon, https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf. Accessed 28 February 2020.

21. Adhikari, Vijay Kumar et al. “A Tale of Three CDNs: An Active Measurement Study of Hulu and Its CDNs.” IEEE, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.387.4423&rep=rep1&type=pdf. Accessed 9 August 2019.

22. D’Hoinne, Jeremy et al. “Critical Capabilities for Cloud Web Application Firewall Services.” Gartner, https://www.gartner.com/en/documents/3970819. Accessed 24 February 2020.



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

REV: 000000