CLOUDFLARE®

Cloud Application Security & Performance: Critical Considerations for SaaS Providers

What SaaS providers need to know about performance, availability, and application security

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

CLOUDFLARE

Executive Summary

Gartner projects that the cloud services industry will grow at nearly three times the rate as overall IT services through 2022, with SaaS comprising the largest segment of this market.[1] SaaS solutions are now an integral component of business infrastructure, but SaaS providers are operating in an increasingly crowded marketplace. An industry survey conducted in the spring of 2018 identified 6,829 SaaS companies competing in the marketing space alone.[2]

To differentiate themselves amidst this intense competition, SaaS providers must rapidly deliver their applications to market and provide end-users with flawless performance, continuous availability, cuttingedge features, and robust data security, all while keeping subscription prices affordable and internal operational costs low.

PART 1

Customers no longer tolerate sluggishness & downtime

At the dawn of the millennium, the human attention span was 12 seconds long; today, it is only eight seconds.[3] This has profound implications not only for marketers and advertisers but also for web developers and SaaS providers. Today's digital consumers demand websites, applications, and APIs that load instantaneously and are never offline. Recognizing this, Google uses page speed as a ranking factor for both desktop and mobile search.[4]

The severity of performance problems vary widely, ranging from a few seconds of delay to the entire application being unresponsive or unavailable. However, even small issues can have a noticeable impact on engagement and conversion rates:

- Google found increased site latency as small as 100-400 milliseconds to have a measurable impact on consumer behavior[5]
- Just one additional second of load time can cause conversions to drop by 7%[6]
- About half of mobile users expect apps to respond in two seconds or less[7]

Optimizing performance & ensuring application availability

A variety of factors can impact SaaS application performance, including the geographic distance between the application's origin server and the end-user, the application's design, seasonal spikes in demand, end-users' internet connectivity, and distributed denial-of-service (DDoS) attacks, where hackers bombard servers with junk requests in an attempt to overwhelm them. There are a variety of methods through which SaaS providers can tackle these challenges.

Content delivery networks (CDNs)

It's estimated that every 100 miles of geographic distance between an app or website's resources and an end user adds 0.82 milliseconds of latency.[8] A content delivery network (CDN) is a geographically distributed group of servers strategically placed at exchange points between different networks. These servers cache static content at the network edge and deliver it to users from the CDN server that is closest to them. The majority of web traffic today is served through CDNs, including traffic from major sites such as Facebook, Netflix, and Amazon.

In addition to improving load times, CDNs provide the following benefits:

- **Reduced bandwidth costs.** By caching static content at the edge and applying other optimizations, such as file compression and minification, CDNs minimize the amount of data that origin servers must provide.
- **Redundancy & reliability.** Because servers are distributed, CDNs can employ load balancing to handle significant spikes in demand, hardware and system failures, and DDoS attacks, ensuring that applications are always available.
- **Improved data security.** CDNs can ensure that applications have fresh TLS/SSL certificates to encrypt and protect data in transit.

Load balancing

Load balancing distributes application traffic across multiple servers to maximize performance. In addition to ensuring that no one server is overloaded, if a server does go down, a load balancer redirects traffic to the remaining servers. Client requests can be distributed sequentially, routed to the server with the fewest connections or, as in the case of a CDN, geo-steered to the server that is closest to the end-user

Adoption of modern web standards

In addition to using a load balancer and delivering assets as geographically close to end-users as possible, SaaS developers should ensure they are using modern web standards such as HTTP/2, TLS 1.3, and IPv6. These standards are more efficient than their predecessors, fix many of the older standards' inherent problems, and include a number of features to reduce latency and enhance performance and data security. For example, TLS 1.3 speeds up the TLS handshake by removing an entire round-trip connection for session establishment; the IPv6 protocol handles packets more efficiently than IPv4; and HTTP/2 allows header compression and multiplexing, among other features.

Content optimization

Modern websites are bulkier than ever; total page size has steadily climbed since at least 2011.[9] All of this heavy, unoptimized static content adds yet more latency, especially on mobile devices, which is where nearly 60% of web searches originate.[10] Content optimization best practices include:

- Responsive design to automatically adjust the way content is delivered depending on the end-user's device.
- Minification to remove unnecessary whitespace, comments and other content in text-based resources, such as JavaScript, CSS, and HTML. This can reduce file size by up to 20%.
- Configuring servers to compress text resources before sending them to users.
- Utilize local storage caching on browsers and mobile devices.
- Defer the loading of JavaScript until text, images, and fonts have been rendered.

PART 2

SaaS applications are major targets for cyber criminals

In the traditional on-premises application deployment model, all data was stored and processed within the end-user's boundary, whether that boundary was a corporate intranet or an individual computer. In contrast, cloud applications and services store, process, and transmit a wealth of sensitive data on the SaaS provider's end, including confidential business information, financial and health data, user login credentials, and personally identifiable information (PII). SaaS providers must ensure that this data is secured from unauthorized access by external hackers, as well as malicious company insiders.

Because many SaaS providers host multiple client applications within a shared infrastructure, any data leaks, reliability incidents, or attacks against that shared infrastructure could negatively affect multiple customers. In 2017, Sabre Corporation disclosed that its SaaS hotel reservations solution, used by more than 32,000 properties, had been breached. The attack exposed credit card data belonging to guests of major hotel brands, including Four Seasons, Loews Hotels, and Hard Rock Hotels & Casinos.[11] Sabre President Clinton Anderson called the breach a "day of awakening."[12]

The potential fallout from a successful cyber attack includes service disruptions, brand degradation, customer churn, losses in revenue, and regulatory fines from being found out of compliance with the GDPR and other legislation requiring businesses to take adequate steps to secure customer data. Class-action lawsuits filed by data breach victims against Uber and MyFitnessPal are currently in arbitration.[13] Because it attempted to cover up the breach, Uber was fined $148 million by U.S. authorities, plus an additional $1.2 million by European authorities. Had the GDPR been in force when the Uber breach surfaced, the company could have been fined 4% of its annual revenue, or about $260 million.[14]

Securing SaaS applications

The potential attack surface for cloud apps is vast and includes login portals, shared DNS and hosting, and application vulnerabilities. SaaS providers can also come under attack from within at the hands of malicious or negligent company insiders.

DDoS attacks

DDoS attacks are growing in frequency, size, and severity. Attacks sized 100Gbps and higher skyrocketed by 967% between Q1 2019 and Q1 2018, and over three-quarters of attacks targeted more than one vector.[15] Many DDoS attacks utilize "zombie armies" of hijacked IoT devices, as was the case in the Mirai botnet attacks against DNS provider Dyn in 2016.[16] Sometimes, hackers will use DDoS attacks as a distraction to tie up security personnel while launching another type of cyberattack.

Effectively mitigating DDoS attacks requires a multi-pronged strategy combining proactive and reactive security measures. Utilizing a CDN network and load balancing absorbs the impact of DDoS attacks by distributing traffic across multiple servers, while traffic filtering measures such as rate limiting, whitelisting/blacklisting IP addresses, and connection tracking blocks malicious requests while allowing legitimate traffic through.

Targeted DNS attacks

DNS attacks involve hackers gaining control of a website's DNS records and redirecting visitors to a malicious site, often one that is designed to look like the original, legitimate site. These attacks can unfold in one of three ways: by installing malware on end-user devices that overrides their DNS configuration; by hijacking a user session on a

public Wi-Fi network; or by stealing login credentials and using them to access a domain name owner's DNS records. When the target of an attack is a SaaS application, the hacker's end goal is generally to steal customer data or hijack customer accounts. According to Verizon, about one-third of reported data breaches likely involved a DNS attack.[17]

The best defense against DNS attacks is to use a secure, managed DNS registration service that makes use of DNSSEC, a set of security protocols that verifies DNS records using cryptographic signatures. By ensuring that a site's signature matches its record, DNS resolvers can authenticate the origin of the data being sent from the DNS server.

Credential stuffing attacks

Credential stuffing attacks make use of the mountains of compromised login credentials available for sale on the Dark Web. Hackers use login software and proxies, often IoT botnets, to bombard websites and SaaS apps with these username/password combinations. Because many people use the same login credentials on multiple sites and apps, it's likely some of them will work.

About 90% of login attempts on eCommerce sites come from credential stuffing; airlines, consumer banks, and hotels are also among the top targets for this type of attack.[18] The attacks will continue to proliferate as long as end-users insist on reusing login credentials. Technical controls against credential stuffing include requiring end-users to solve CAPTCHAs and deploying rate limiting, which blocks attacks at the network edge by defining custom rules that set request thresholds, timeout periods, and response codes.

Insider threats

External hackers aren't the only threats to SaaS application security. Malicious insiders who purposefully misuse their access to company resources, as well as negligent insiders who disregard security and access policies, pose serious threats to data security. A study released by Nucleus Cyber in July 2019 reported that 60% of organizations had experienced at least one insider attack over the previous 12 months.[19]

SaaS providers must set user access to internal applications on a granular basis, employing the principle of least privilege; each employee should be granted the minimum system access that they need to perform their job, and no more. Additionally, they must protect against credential theft by implementing user authentication procedures such as multi-factor authentication (MFA) and continuously monitoring systems for anomalous behaviors.

Malicious payload exploits

Malicious payloads exploit application vulnerabilities using methods such as SQL injections, cross-site scripting, and remote file inclusions to expose sensitive data. SaaS providers must protect their applications by deploying a web application firewall (WAF) to identify and block malicious requests. Because the cyber threat environment is dynamic, WAF rules must be updated frequently to ensure applications are protected from new and emerging threats.

Interception of unencrypted customer data

In addition to being exfiltrated from the SaaS application itself, customer data is also vulnerable while in transit, which is why all communications between the application and its end-users must be encrypted.

SSL is no longer optional, but enabling it on CNAME domains is tricky

SSL (Secure Sockets Layer) is a standard security protocol that establishes an encrypted link between a server and a client, such as a browser and a web server (website). The modern version of the protocol is called TLS (Transport Layer Security). A website that uses SSL (TLS) will have an HTTPS web address.

Without SSL, any data transmitted between the browser and the web server is sent in plain text, which means that hackers can easily intercept it in transit. To prevent this from happening, websites obtain an SSL certificate. This is a "digital passport" that associates the web server with a cryptographic key and initiates a secure session with the user's browser, ensuring that any communications between the browser and the server are encrypted.

In the early days of SSL, only certain pages on a website were encrypted, such as eCommerce shopping carts. However, in recent years, major tech companies have exerted increasing pressure on web developers and SaaS providers to universally adopt HTTPS. Google began using HTTPS encryption as a ranking signal in 2014.[20] Then, Google Chrome and other popular web browsers began displaying prominent warnings on websites served over HTTP connections, advising visitors that they were not secure.[21] As a result of these moves, SSL (TLS) encryption is now a de facto requirement to conduct business online.

However, as the web embraced SSL, an important subset of businesses were left behind: SaaS providers that offer their customers the ability to use white-labeled vanity domains for public-facing online assets, such as landing pages, websites, and support portals.

SaaS providers typically host customer assets on a subdomain of their primary domain: for example, customercompany.saasprovider.com. However, most customer companies do not want this URL to be visible to their own end-users; because the URL includes another company's name, leaving it visible would dilute their brand, confuse their end-users, and damage their SEO. Instead, they use their own, branded URL, such as customercompany.com or support.customercompany.com, and use a CNAME to point it to customercompany.saasprovider.com.

Unfortunately, it is extremely difficult to enable SSL on CNAME domains. SaaS providers have traditionally had only two options. The first was to ask their customers to set up a reverse proxy on their servers to secure the connection, then forward the request to the SaaS provider's server. However, this requires a tremendous amount of time, effort, and technical expertise on the customer's part.

The second option was for the SaaS provider to build an automated or manual in-house solution, which requires a tremendous amount of time and effort on the part of the SaaS provider, the customer, or both. Additionally, the SSL certificates must be deployed on a large-scale global distribution network and continuously maintained, requiring further time, effort, and expense.

PART 3

Cloudflare's solutions for SaaS application performance & security

Cloudflare enables SaaS providers to rapidly deliver secure, high-performance applications, minimize their operational costs, and differentiate themselves in a crowded marketplace.

Performance, availability, and content optimization

The Cloudflare network of data centers spans cities around the world. Each data center supports the full stack of Cloudflare performance and security services to optimize web performance across its network. From fast web address lookups to accelerated delivery to the origin server, Cloudflare speeds up traffic at key points in the life of a request.

Cloudflare DNS is the world's fastest and most reliable authoritative DNS provider.[22] Cloudflare provides fast and secure managed DNS as a built-in service on its network.

Cloudflare **CDN** spans a global network of data centers that cache content closer to users so that requests don't need to travel long distances to origin servers, minimizing latency.

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.

Cloudflare supports the **latest web standards** and protocols, including HTTP/2 and QUIC (HTTP/3) for faster application layer data transmission, TLS 1.3 for more efficient SSL encryption.

Cloudflare Argo Smart Routing delivers dynamic web content over the fastest links available, resulting in noticeably faster delivery and improved end-user experience.

Cloudflare supports the use of **Signed Exchanges with Google AMP**, providing native URL attribution when viewed in the AMP viewer.

For mobile apps, the **Cloudflare Mobile SDK** provides mobile network performance analytics that can be integrated into any app.

Cloudflare offers a number of **image optimization** features, including Image Resizing, Polish, and Mirage. Image Resizing allows customers to optimize images by resizing, cropping, compressing, or converting them to WebP, a newer image format designed for fast loading. Cloudflare also enables **parallel streaming of progressive images** to speed up delivery of multiple images on a page.

Cloudflare offers several options for optimizing video. **Cloudflare Stream** is an online video platform for streaming media, and **Stream Delivery** ensures videos stream as fast as possible. Cloudflare offers **Concurrent Streaming Acceleration** for live streaming content as well.

Prioritization, or the order in which the assets on a web page are loaded, makes a huge difference to page load speed. **Rocket Loader** from Cloudflare optimizes the prioritization of any assets that need to load before on-page JavaScript can execute. Cloudflare also supports **HTTP/2 Prioritization** in order to control how page assets are prioritized, avoiding the slower default prioritization of most browsers. **BinaryAST for JavaScript** is supported by Cloudflare to speed up JavaScript parsing so that it executes faster – crucial for the performance of dynamic or personalized web pages.

Application & data security

All Cloudflare plans offer unlimited, unmetered **mitigation of DDoS attacks**, regardless of the size of attack. Cloudflare's layered security approach combines multiple DDoS mitigation capabilities into one service, preventing disruptions caused by bad traffic while allowing good traffic through. With 30 Tbps of capacity, Cloudflare's global network can handle any modern distributed attack, including those targeting DNS infrastructure.

Cloudflare DNS uses DNSSEC to verify DNS records using cryptographic signatures, protecting SaaS applications from DNS attacks. Cloudflare also offers **1.1.1.1**, which is a public DNS resolver that keeps DNS queries private.

Cloudflare offers granular control through **rate limiting** to detect and block credential stuffing attacks at the network edge, along with Cloudflare **Bot Management** to detect malicious bots used for credential stuffing and other cyber attacks, such as content spam and inventory hoarding.

Cloudflare Access helps SaaS providers mitigate insider threats by allowing them to secure, authenticate, and monitor user access to any domain, application, or path on Cloudflare on a granular level. Cloudflare Access also provides full visibility into recent logins, access requests, and policy changes so that security personnel can monitor for suspicious or anomalous behavior.

Cloudflare's enterprise-class **web application firewall (WAF)** protects SaaS applications from common application vulnerability attacks, including SQL injection, cross-site scripting, and cross-site forgery requests. Cloudflare's WAF keeps applications continuously protected against new and emerging threats through automatic updates.

Cloudflare's **SSL for SaaS** makes it easy for SaaS providers to enable SSL (TLS) on their customers' CNAME vanity domains and frees SaaS providers and their customers from the burden of SSL certificate management. Additionally, Cloudflare's solution significantly improves performance over in-house solutions by terminating SSL as physically close to web visitors as possible.

Rapid delivery of applications to market

Serverless computing has great potential for creating faster, more responsive apps than ever by allowing developers to write and deploy code without consideration of the underlying infrastructure. **Cloudflare Workers** allows developers to build serverless applications that run on Cloudflare's network, closer to your users. Applications built with Cloudflare Workers are always available, with low-latency responsiveness.

Endnotes

1. “Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019,” Gartner Newsroom, https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-publiccloud-revenue-to-g. Accessed August 6, 2019.

2. Smale, Thomas. “4 Issues Facing the Saas Industry in 2019,” SaaS Magazine, https://saasmag.com/4-issues-facing-the-saas-industry-in-2019/. Accessed August 6, 2019.

3. The Human Attention Span [Infographic], Digital Information World, https://www.digitalinformationworld.com/2018/09/the-human-attention-span-infographic.html. Accessed August 6, 2019.

4. “Using page speed in mobile search ranking,” Google Webmaster Central Blog, https://webmasters.googleblog.com/2018/01/using-page-speed-in-mobile-search.html. Accessed August 6, 2019.

5. Brutlag, Jake. “Speed Matters,” Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html. Accessed August 6, 2019.

6. Rodman, Tedd. “Marketing & Web Performance: How Site Speed Impacts Metrics,” Yotta, https://www.yottaa.com/marketing-web-performance-101-how-site-speed-impacts-your-metrics. Accessed August 6, 2019.

7. Dimensional Research. “Failing to Meet Mobile App User Expectations: A Mobile App User Survey,” https://techbeacon.com/sites/default/files/gated_asset/mobile-app-user-survey-failing-meet-userexpectations.pdf. Accessed August 6, 2019.

8. Sherman, Fraser. “Network Latency Milliseconds Per Mile,” Techwalla, https://www.techwalla.com/articles/network-latency-milliseconds-per-mile. Accessed August 6, 2019.

9. Report: State of the Web, HTTP Archive. http://beta.httparchive.org/reports/state-of-the-web#bytesTotal. Accessed August 6, 2019.

10. Sterling, Greg. “The mobile, desktop split may have stabilized at roughly 60% – 40%,” Search Engine Land, https://searchengineland.com/mobile-desktop-search-traffic-split-may-have-stabilized-atroughly-60-40-317091. Accessed August 6, 2019.

11. Hertzfeld, Esther. “New hotels caught in Sabre's data breach,” Hotel Management, https://www.hotelmanagement.net/tech/sabre-s-data-breach-affects-new-hotels. Accessed August 6, 2019.

12. Taylor, Ian. “Sabre breach ‘a wake-up call’, ITB hears,” Travel Weekly, http://www.travelweekly.co.uk/articles/326108/sabre-breach-a-wake-up-call-itb-hears. Accessed August 6, 2019.

13. “MyFitnessPal Data Breach Lawsuit Sent to Arbitration,” JD Supra, https://www.jdsupra.com/legalnews/myfitnesspal-data-breach-lawsuit-sent-49746/. Accessed August 6, 2019.

14. Jones, Rhett. “Uber's Mountain of Data Breach Fines Just Got $1.2 Million Higher,” Gizmodo, https://gizmodo.com/uber-s-mountain-of-data-breach-fines-just-got-1-2-mill-1830679083. Accessed August 6, 2019.

15. 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.

16. Dignan, Larry. “Dyn confirms Mirai botnet involved in distributed denial of service attack,” ZD Net, https://www.zdnet.com/article/dyn-confirms-mirai-botnet-involved-in-distributed-denial-of-service-attack/. Accessed August 6, 2019.

17. Global Cyber Alliance, “The Economic Value of DNS Security,” https://www.globalcyberalliance.org/wpcontent/uploads/Economic-Value-of-DNS-Security-GCA-2019.pdf. Accessed August 6, 2019.

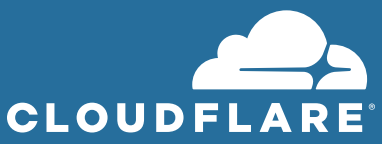
18. Detrixhe, John. “Hackers account for 90% of login attempts at online retailers,” Quartz, https://qz.com/1329961/hackers-account-for-90-of-login-attempts-at-online-retailers/. Accessed August 6, 2019.

19. Bayern, Macy. “60% of companies experienced insider attacks in the last year,” TechRepublic. https://www.techrepublic.com/article/60-of-companies-experienced-insider-attacks-in-the-last-year/. Accessed August 6, 2019.

20. “HTTPS as a ranking signal,” Google Webmaster Blog, https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html. Accessed August 6, 2019.

21. “Safari Says: Not Secure. What Does It Mean?" macReports, https://macreports.com/safari-says-notsecure-what-does-it-mean/. Accessed August 6, 2019.

22. “DNS Performance Analytics and Comparison." DNSPerf, https://www.dnsperf.com/. Accessed 23 July 2019.



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

REV: 041620