CLOUDFLARE®

5 Ways to Maximize the Security, Performance and Reliability of Your Online Business

The Internet is changing rapidly, and with it, so is the nature of modern enterprises. Providing a superior online experience for a global customer base is no longer optional; as demand increases for web-based services and applications, businesses must rise to satisfy customer needs while ensuring that their websites and applications remain as secure, fast, and reliable as possible.

With this shift to digital transformation, enterprises face new challenges and opportunities for growth — from anticipating and meeting customers' digital needs to mounting a strong defense against web-based attacks, overcoming latency issues, preventing site outages, and maintaining network connectivity and performance.

When optimizing the online customer experience, enterprises need to adopt a strategy that integrates robust site security, performance, and reliability. Although this strategy involves many components, here are five key considerations that can help businesses meet customer needs and provide a secure and seamless user experience.

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

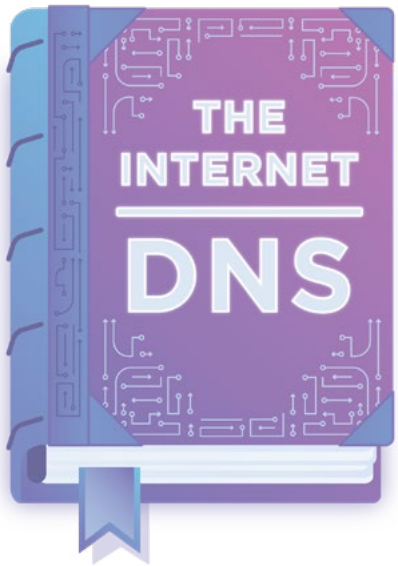
Leverage DNS and DNSSEC support to maximize availability and uptime

Frequently referred to as the 'phone book of the Internet,' DNS (domain name system) translates domain names into numeric IP addresses and enables browsers to load Internet resources. Since DNS is designed to accept any address given to it, selecting the right DNS security strategy is crucial. Without it, businesses are exposed to several risks, including DNS hijacking, man-in-the-middle attacks, the exposure and loss of sensitive user information, phishing, and other major threats. As DNS attacks become more prevalent, businesses are starting to realize that a lack of a resilient DNS creates a weak link in their overall security strategy.

There are multiple approaches that companies can take to deploy a resilient DNS strategy. They can get a managed DNS provider that hosts all DNS records, offers query resolution at multiple nodes globally, and provides integrated DNSSEC support. DNSSEC adds a layer of security to the domain name system by adding cryptographic signatures to existing DNS records. Companies can also build additional redundancy by deploying a multi-DNS strategy — even if the primary DNS goes down, secondary DNS helps keep the applications online. Large enterprises that prefer to maintain their own DNS infrastructure can implement a DNS firewall in conjunction with a secondary DNS. This setup adds a security layer to the on-prem DNS infrastructure and helps ensure overall DNS redundancy.

Customer success story

A cryptocurrency firm that provides an open-source, client-side tool for interacting with the blockchain needed to boost their DNS security after a sophisticated DNS attack rerouted all queries to an imposter website. Hackers managed to convince one of the authoritative servers that all queries for the firm's website should be directed to a new destination. The imposter website looked identical to the firm's site, but used the dupe to transfer the users' private keys to hackers, effectively giving attackers access to a massive amount of cryptocurrency.



Like many websites on the internet, they were targeted because of a major vulnerability in the Internet's core infrastructure, and lost their customers' trust as a result. To make sure it never happened again, they adopted Cloudflare DNS. Moving to Cloudflare was the most straightforward way to implement DNSSEC, as they were able to provision and manage the protocol from a unified, easy-to-use dashboard — not only improving the resiliency of their security landscape, but ensuring a more secure and efficient user experience for customers who depended on them to safeguard their crypto assets.

For more information on DNS and DNSSEC integration, visit Cloudflare DNS.

Accelerate content delivery by routing traffic across the least-congested routes

Today, the majority of web traffic is served through Content Delivery Networks (CDNs), including traffic from major sites like Amazon and Facebook. A CDN is a geographically distributed group of servers that help provide fast delivery of Internet content to globally dispersed users and can also reduce bandwidth costs.

With servers in multiple locations around the globe, a CDN is able to distribute content closer to website visitors, and in doing so, reduce any inherent network latency and improve page load times. CDNs also serve static assets from cache across their network, reducing the number of requests being made to hosted web servers and resulting in lower bandwidth and hosting costs.

Customer success story

This was one of the issues plaguing one of the largest on-demand food delivery services in the world. With partners in thousands of cities across the U.S. and a door-to-door service that depends on their online platform and smartphone apps, it is essential that they provide a fast, reliable user experience at all times.

This not only helps support a growing user base, but strengthens their partnerships with local restaurants and merchants as well.

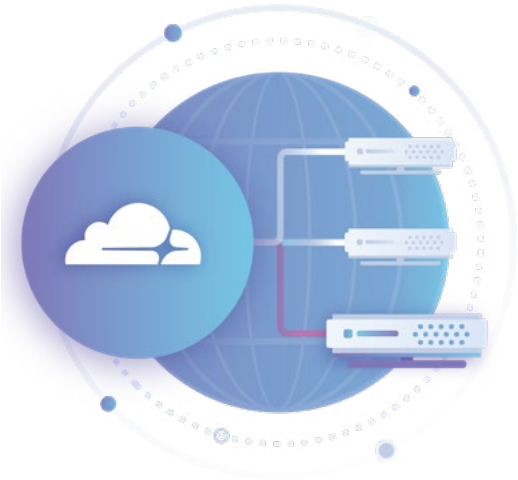
Initially, the company was facing several performance challenges. They lacked a resilient CDN and image resizing solution, the latter of which was key to their ability to provide a smooth user experience. Customers visiting the site needed to be able to browse high-res photos of different food options, and as the company grew, the number of menu items they presented to their users increased as well. With a high volume of high-quality images served via their platform, finding a solution to optimize image delivery and decrease latency was vital, especially as their previous image resizing solution was costing them thousands of dollars per month.

Cloudflare helps the food delivery provider accelerate their user experience with the Cloudflare Content Delivery Network (CDN). Backed by a global network spanning 25+ million Internet properties, the Cloudflare CDN caches static content as close to end users as possible and works in tandem with Argo Smart Routing to intelligently route content requests along the fastest path. And, with Cloudflare Image Resizing empowering the company to cache images and reduce latency, their CPU utilization decreased by 20%.

To find out how a CDN can accelerate content delivery for your business, visit Cloudflare CDN.

Minimize the risk of site outages by globally load balancing traffic

Maximizing server resources and efficiency can be a delicate balancing act. Servers that become overloaded or are too geographically distant from end users can have a detrimental effect on business, as increased latency and server failure can result in lost revenue, broken customer trust, and brand degradation.



Cloud-based load balancers distribute requests across multiple servers in order to handle spikes in traffic. The load balancing decision takes place at the network edge, closer to the users — allowing businesses to boost response time and effectively optimize their infrastructure while minimizing the risk of server failure. Even if a single server fails, the load balancer can redirect and redistribute traffic among the remaining servers, ensuring that customers never experience significant latency or see a site outage. The load balancer also allows for active health checks, which allows businesses to identify underperforming servers and take preemptive measures before a breakdown actually occurs.

Customer success story

When a large Canadian-headquartered ecommerce platform — operating from 175 countries around the world — needed an integrated performance and security solution, they looked for a provider that would ensure ease of implementation and help them curb infrastructure costs. During the company's migration to Cloudflare, they needed the process to be seamless, without interrupting any of the 1+ million businesses that depended on its platform. By placing each of the sites on Cloudflare's global network, the ecommerce company empowered their merchants with a faster experience for their customers that helped drive increased sales across the platform.

A central part of these performance benefits was Cloudflare Load Balancing, which allowed the company to utilize dynamic steering — in other words, direct traffic to the fastest origin server pool for a given user, diminishing latency and speeding up traffic even more. Now, the company has granular control over how their traffic is distributed between origin servers, with the added performance and accuracy benefits of making these decisions at the network edge.

Learn how to improve application performance and availability with Cloudflare Load Balancing.

Protect web applications from malicious attacks

The Internet exposes web-based businesses to a vast spectrum of attacks from different locations and with various levels of complexity. When securing web applications and other business-critical properties, a layered security strategy can help defend against many different kinds of threats.

Web application firewall protection

A web application firewall, or WAF, protects web applications by filtering and monitoring HTTP traffic. With a WAF in place, businesses can protect against zero-day attacks and shield their applications against common threats like cross-site request forgery (CSRF), cross-site scripting (XSS), and SQL injection attacks — which may compromise servers and allow data theft or tampering.

A WAF also enables businesses to maintain granular control over their security policies by setting rules that can protect vulnerabilities in their applications and mount a defense against emerging threats. Cloud-based WAFs are typically the most flexible and cost-effective solution to implement, as they can be consistently updated to protect against new threats without significant additional work or cost on the user's end.

Customer success story

For a Fortune 500 multinational financial corporation, onboarding additional marketing websites for each geographic location presented a challenge. The corporation needed to establish a global online presence, but was forced to outsource complex configuration or pay for expensive professional services with their previous provider — a process that proved time intensive and cost prohibitive. They needed a modern architecture solution that would grant them more granular control over their web properties and help them balance a multi-cloud approach between their on-premise data centers and cloud-based applications.

After switching to Cloudflare, the company was able to protect over 700+ web properties within minutes — without any additional expense. Now, they can reap the benefits of a more flexible, self-serve environment, saving both time and precious internal resources.

Since many of the company's websites allow banks to access digital card services and handle other sensitive data, adopting a layered security strategy is a top priority for the institution. Even a single successful attack could compromise their brand reputation and damage their trust with vendors and customers. With the Cloudflare Web Application Firewall (WAF) and Advanced DDoS Protection in place, every site is shielded from incoming attacks and malicious threats.

Learn how to protect business-critical web applications from malicious attacks with the Cloudflare Web Application Firewall.

DDoS attack protection

For most websites, a high volume of web traffic can be a good thing, leading to more conversions, customers, and sales. However, spikes in web traffic can also stem from cyber attacks intended to disrupt network connections, overwhelm servers, and prevent legitimate users from accessing a site.

A DDoS attack is a malicious attempt to overburden servers, devices, networks, or surrounding infrastructure with a flood of illegitimate Internet traffic. By consuming all available bandwidth between targeted devices and the Internet, these attacks not only cause significant service disruptions, but have a tangible and negative impact on business as customers are unable to access a business's resources.

Customer success story

India's largest ticketing company has over 60 million customers and sees around five billion screen views per month, with 200+ million tickets sold over a year. Providing a fast and secure user experience is paramount to the success of their services, as a negative experience can drive customers to another competitor. When the company experienced a massive DDoS attack, it posed a substantial risk to their platform.

With Cloudflare Advanced DDoS Protection in place, they didn't have to go into 'panic mode' in order to mitigate the attack. With over 35 Tbps of network capacity, Cloudflare's DDoS protection is designed for ease of use and management, and blocks attacks at the network edge to keep origin servers up and available — whether they're located in an on-premise, hybrid, or multi-cloud environment.

Cloudflare instantly began blocking the malicious traffic — up to 50 gigabytes per second — and effectively prevented the DDoS attack from disrupting operations or slowing down the site. That allowed the ticketing company to not only improve its security posture, but ensure total reliability and operational efficiency moving forward.

For more information on adopting a layered security approach, visit Cloudflare Advanced DDoS Protection.

Malicious bot mitigation

Fully securing customer data and web applications against cyber threats requires a layered approach.

In addition to other common cybersecurity threats, sites may become compromised when targeted by malicious bot activity, which can overwhelm web servers, skew analytics, prevent users from accessing webpages, steal user data, and compromise critical business functions.

Good bots refer to software applications that are programmed to perform useful tasks, from scanning content on webpages to responding to customer inquiries on a website. However, bots can also become compromised by hackers and used to perform malicious activities, from credential stuffing and breaching sensitive data to stealing SEO content and disrupting business operations. By implementing a bot management solution, businesses can distinguish between useful and harmful bot activity and prevent malicious behavior from impacting user experience.

Customer success story

An industry leader in marketing automation software ran into this problem when their web forms were inundated with spam bot activity. Bots frequently targeted the forms and made it nearly impossible for legitimate users to access the pages quickly and easily, compromising the company's ability to provide a seamless experience for their customers.

The company turned to Cloudflare for a bot mitigation solution that would allow them to block malicious requests without degrading their user experience. Cloudflare Bot Management uses machine learning to detect anomalies in web traffic patterns and block bot attacks and malicious traffic, while still permitting good bots and legitimate traffic to pass through. Today, Cloudflare helps them mitigate over 1 million malicious bot requests per day, enabling their users to utilize their marketing software without running the risk of a disruption of service or loss of sensitive data.

Mitigate bot attacks and manage good and bad bots in real-time with Cloudflare Bot Management.

Keep your network up and running

Protect your network infrastructure

It's not enough to just protect web servers. Enterprises often have on-premise network infrastructure hosted in public or private data centers that needs protection from DDoS attacks, too. Many DDoS mitigation providers rely on one of two methods for stopping an attack: scrubbing centers or on-premise scanning and filtering via hardware boxes. The problem with both approaches is that they impose a latency penalty that can adversely affect a business.

Scrubbing requires re-routing network traffic to centralized scrubbing servers in designated geographic locations in an attempt to filter or 'scrub' out malicious traffic from non-malicious traffic. Re-routing all traffic to a geographically distant scrubbing center incurs additional latency which is often unacceptable for most applications.

Another DDoS mitigation technique uses on-premise hardware boxes to scan traffic and filter out malicious requests. Similar to scrubbing, the scanning hardware introduces network latency and inhibits performance due to the bottleneck nature of re-routing network traffic through the boxes to complete the scanning process. On-premise anti-DDoS appliances often have a bandwidth limit by default, which is based on the combination of the organization's network capacity and the box's hardware capacity.

A better way to detect and mitigate DDoS attacks is to do so close to the source — at the network edge.

By scanning traffic at the closest data center in a global, distributed network, high service availability is assured, even during substantial DDoS attacks. This approach reduces the latency penalties that come from routing suspicious traffic to geographically distant scrubbing centers. It also leads to faster attack response times.

Customer success story

When the nonprofit organization running one of the top 10 Alexa-ranked websites suffered severe latency and site outages, they needed a solution that would mitigate attacks at the network layer and get them back online fast.

Characterized as a 'takedown attack' — a malicious attempt that overwhelms a company's servers and effectively shuts down all operations — the attack flooded the servers with illegitimate network layer and HTTP traffic. The company called on Cloudflare to mitigate the attack and restore access to their site, while also implementing network layer DDoS protection that would help prevent future attacks.

Cloudflare Magic Transit provides DDoS protection for on-premise networks and data centers, either in always-on or on-demand deployment modes. It uses Cloudflare's global network to detect and mitigate DDoS traffic in the Cloudflare data centers closest to attack sources. With Cloudflare's large-scale network and robust DDoS protection in place, the company was able to quickly circumvent the effects of the attack, restoring end-user experience back to normal levels.

Visit Cloudflare Magic Transit to learn more about network DDoS protection.

Protect TCP/UDP applications

At the transport layer, attackers may target a business's server resources by overwhelming all available ports on a server. These DDoS attacks can cause the server to respond slowly to legitimate requests — or not at

all. Preventing attacks at the transport layer requires a security solution that can automatically detect attack patterns and block attack traffic.

Customer success story

This was one of the issues facing an esports industry leader and game producer — one that boasts over 200 million global users — when they detected numerous DDoS attacks and discovered that some of their users in remote parts of the globe were encountering poor user experience on their TCP-based applications. In the gaming industry, those represent sizable setbacks, since any service downtime can lead to a massive loss of customers and revenue.

The game provider's infrastructure operates over a proprietary network protocol designed for the low-latency demands of gamers — so when it comes to DDoS attacks, conventional security products aren't able to safeguard these custom protocols.

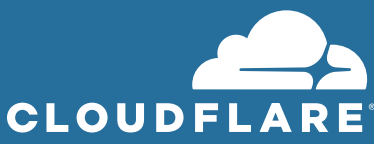
In order to boost performance and mitigate DDoS attacks at the transport layer, the company enlisted the help of Cloudflare. Cloudflare Spectrum — DDoS protection for any TCP/UDP protocols — allows them to protect their critical custom communication protocol without impairing end-to-end performance, successfully thwarting attempts to slow down their service and damage their brand reputation. In addition, Cloudflare Spectrum also uses TCP optimizations and Argo Smart Routing to accelerate TCP traffic over the Cloudflare network.

Improve the speed, security, and reliability of your business's TCP/UDP applications with Cloudflare Spectrum.

Conclusion

Creating a superior online experience requires the right security and performance strategy — one that not only enables enterprises to accelerate content delivery, but ensures network reliability and protects their web properties from site outages, data theft, and other critical attacks.

Backed by a network that spans 200+ cities in over 90 countries around the world, Cloudflare provides a scalable, integrated global cloud platform that helps businesses deliver security, performance, and reliability for their on-premise, cloud, and SaaS applications. To learn how you can protect and secure your online business, visit Cloudflare.com.



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

REV: 200330