CLOUDFLARE®

How Financial Organizations Can Maximize Security, Performance and Reliability For Their Online Business

Providing a superior online experience is no longer optional. As demand increases for web-based services and applications, financial services companies must ensure that those websites and applications remain as secure, fast, and reliable as possible.

Beyond this broad trend, several trends make online customer experiences a particularly pressing challenge for financial services companies in particular. The industry has long been a prime target for DDoS attacks at the application and network layers. Such attacks are always increasing in volume and sophistication, posing increased risks to site and application availability.

In addition, shifts and spikes in Internet traffic are becoming more extreme, leading to increased pressure on both edge and network infrastructure. What can companies do to ensure customers retain instant access to their money and financial data, regardless of network congestion or surges in demand?

The answer involves many components. Here are five key considerations that can help any financial services organization get started.

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

An online platform for banking and insurance products faced performance challenges as it expanded from its original home, Singapore, into less-mature Asian markets. Slower local networks and unstable infrastructure impacted the customer experience, hampering the company during a period of critical growth. They started looking for a solution that would reduce load times for their end users across geographies.

Cloudflare's CDN helps them deliver a superior performance across the board, despite varying levels of digital maturity in the end markets. Cloudflare's network spans over 200 cities in 90 countries around the world, ensuring the company's content can be delivered quickly to customers no matter where they are or which device they are using. In addition, Cloudflare's Argo Smart Routing solution uses up-to-the-second intelligence from across its network to route content around congestion, insulating the company from problems with local infrastructure.

Moving to Cloudflare has helped the company enjoy bandwidth cost savings of approximately 75% and a 50% improvement in site performance.

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

https://www.cloudflare.com/case-studies/sureprep-taxes-load-balancing-waf/

This company, a provider of tax preparation software for CPA firms and individual taxpayers, had long used an in-house load balancing solution to preserve uptime. Unfortunately, their existing solution was not scalable — making it hard to address the spikes in traffic during the annual tax filing season. In addition to the scalability challenges, managing their in-house load balancer was a labor-intensive task that their CTO often had to manage himself.

Cloudflare turned out to be an ideal fit for this tax software company. With Cloudflare Load Balancing, this company was able to manage traffic across multiple servers during the peak tax season, achieving 100% uptime and superior performance for their users. Also, they were able to set up the Cloudflare solution with a few clicks — ensuring smooth transition from their previous in-house solution. Cloudflare's unified and intuitive dashboard vastly reduced the time the company spent maintaining their infrastructure, freeing up engineering and IT time for more business-critical tasks.

“Using Cloudflare's load balancer, we were able to manage 35-40 web servers effectively and quickly during our busy season without any fear of messing things up, all through the Cloudflare interface,” the company's CTO notes. “Now I can delegate load balancing to someone else and they can handle it easily.”

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.

A. 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.

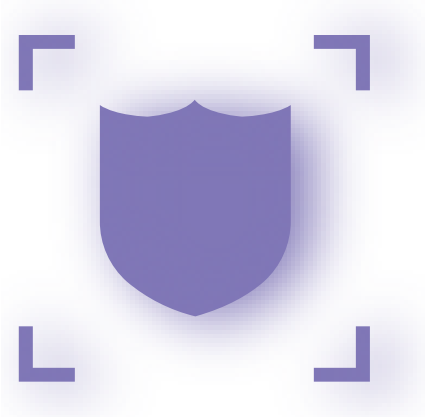
After switching to Cloudflare, the company was able to protect over 700+ web properties within minutes — without any additional expense. Now, they can reap the benefits of a more flexible, self-serve environment, saving both time and precious internal resources.

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.

B. 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

For the world's largest bitcoin trading platform, protecting its high frequency trades from disruption caused by DDoS attacks posed a paramount challenge. A breach in security meant service downtime — every second of which resulted in lost revenue since millions of trades could not be executed. Not only that, downtime impacted customer retention — if a customer could not trade with them, they would go elsewhere to complete the trade.

With Cloudflare's unlimited and unmetered DDoS protection, this bitcoin trading platform got the peace-of-mind ensuring they don't have to worry about their platform being unavailable or compromised. Fueled by the threat intelligence from over 26 million web properties, Cloudflare is able to protect this trading platform against the most sophisticated attacks. 30 Tbps of network capacity allows Cloudflare to handle any modern distributed attack, including those targeting DNS infrastructure.

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

C. 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

https://www.cloudflare.com/case-studies/sofi-overcomes-malicious-traffic-with-cloudflare/

A US-based leading online personal finance company was facing a constant threat from malicious bots. Since its inception in 2011, the company had funded over $40 billion in loans and had more than 800,000 members on its platform. In 2019, the company found itself under an increasing number of credential stuffing attacks from bad bots. These attacks posed a threat to its business and reputation. Mitigating these attacks to protect customer experience and sensitive data was the top of mind concern for the company's executives.

Cloudflare Bot Management helped this personal finance company mitigate credential stuffing attacks in no time. The company's engineers were quickly able to build and deploy granular rule sets and were successful in reducing malicious traffic by over 60%, with a significantly low false-positive rate. In the words of their security engineer — "The great thing about Cloudflare Bot Management solutions is I don't need to spend time fine tuning it. The machine learning algorithms to detect credential stuffing attacks just work because Cloudflare has such great data. Our lives are 1000 times easier while still ensuring our sites are both safe and fast for our customers."

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

Keep your network up and running

A. 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 a large Fortune 500 financial services organization suffered from a ransomware DDoS attack, 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 traffic.

The company called on Cloudflare to activate Magic Transit, which provides DDoS protection for on-premise networks and data centers. Using Cloudflare's global network, Magic Transit detects and mitigates DDoS traffic in the Cloudflare data centers closest to attack sources — without having to redirect traffic to a small number of distant 'scrubbing centers.'

Thanks to this protection, the company was able to quickly mitigate the attack, restore access to their networks, and restore the end-user experience back to normal levels. In addition to the DDoS protection provided, Cloudflare's fixed pricing (regardless of the number or size of attacks) and focus on fast routing was a major edge over other legacy vendors.

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

B. 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.

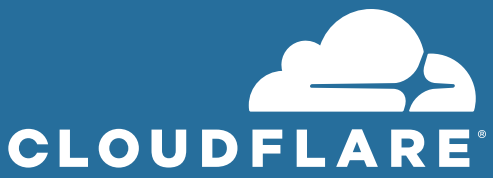
Customer success story

This company, a leading technology provider for cryptocurrency exchanges, payment processors, and brokerage firms, faced a unique challenge in protecting and accelerating its traffic routed over a proprietary TCP protocol. Given the nature of their business, reliability and speed were crucial — a few additional milliseconds was enough to derail transactions on their way to the interbank market.

Cloudflare Spectrum provided them a solution to protect and accelerate all kinds of TCP traffic, including custom protocols. With Cloudflare Spectrum, the company could safeguard the connections using TLS 1.3 with zero-round trip resumption support, enabling fast and secure transit.

By routing its TCP traffic through Spectrum, this company was able to safeguard its production systems from DDoS attacks, while simultaneously ensuring reliability and faster connectivity. The company saw an immediate reduction of over 50% in latency from certain regions. Overall, more than 5TB per month of the company's data is encrypted, protected, and accelerated by Cloudflare.

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