EBOOK

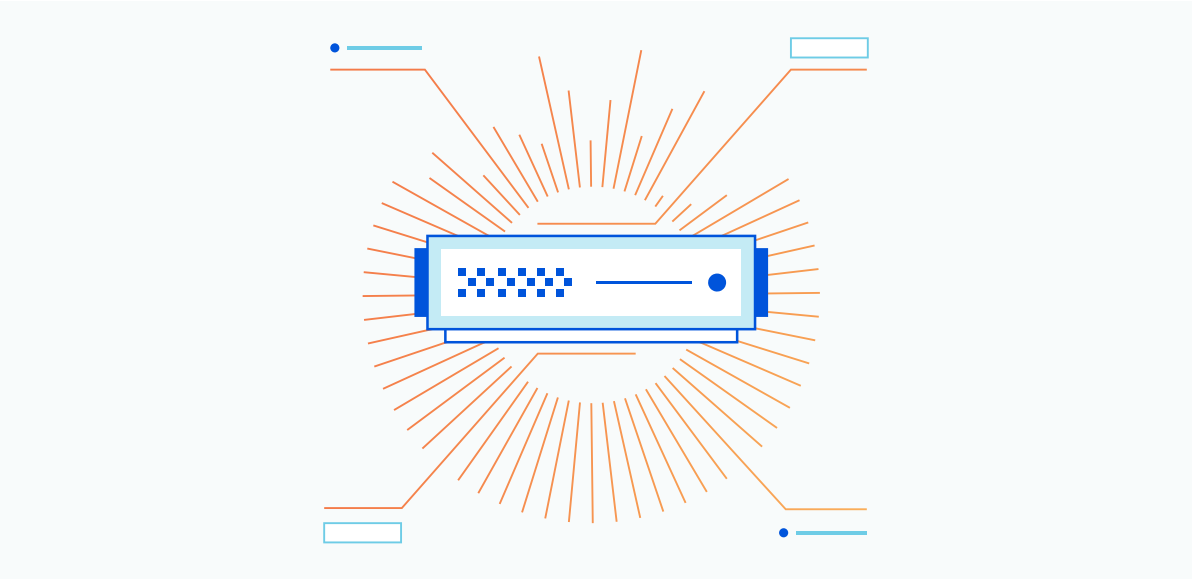
CLOUDFLARE

6 ways startups can maximize security, performance, and reliability for their online business

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

INDEX

INTRODUCTION



Delivering excellent online experiences to customers is essential to growing a startup. To create online experiences that will lead to happy customers and business growth, startups need secure and high-performing websites and/or applications.

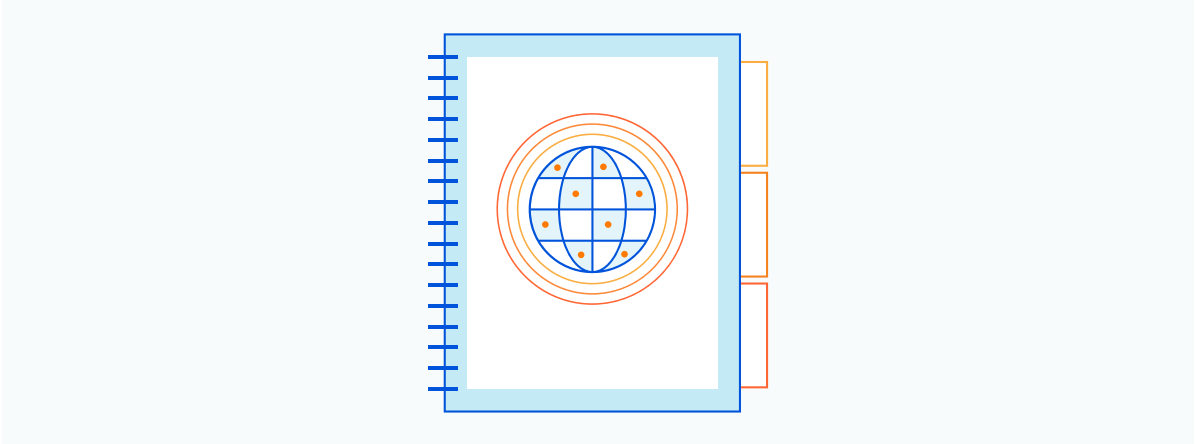
However, there are many components involved in creating and delivering a positive online experience. Like all businesses, startups must anticipate and meet customers' digital needs, mount a strong defense against web-based attacks, overcome latency issues, prevent site outages, and maintain network connectivity and performance.

At the same time, startups face the unique pressure of responding to the fundamental questions and challenges of growing a business. These challenges include everything from raising capital to refining their market positioning.

Fortunately, there are many ways to protect and accelerate Internet properties. Startups generally have limited time and resources, so an integrated approach is best. Easy to use, comprehensive solutions reduce the complexities and data silos that come with managing multiple providers. Moreover, the right solution can help startups deliver excellent online experiences while also saving them time and effort so they can focus on growing their business.

Using the following tips, startups can maximize security, performance, and reliability and ultimately deliver excellent online experiences that will help grow their business.

TIP #1



Secure your DNS to prevent costly attacks

Frequently referred to as the 'phone book of the Internet,' the DNS (domain name system) translates domain names into numeric IP addresses so browsers can load Internet resources. Almost all web traffic requires DNS queries, but without a secure DNS, these requests leave businesses vulnerable to attacks. Common DNS attacks include:

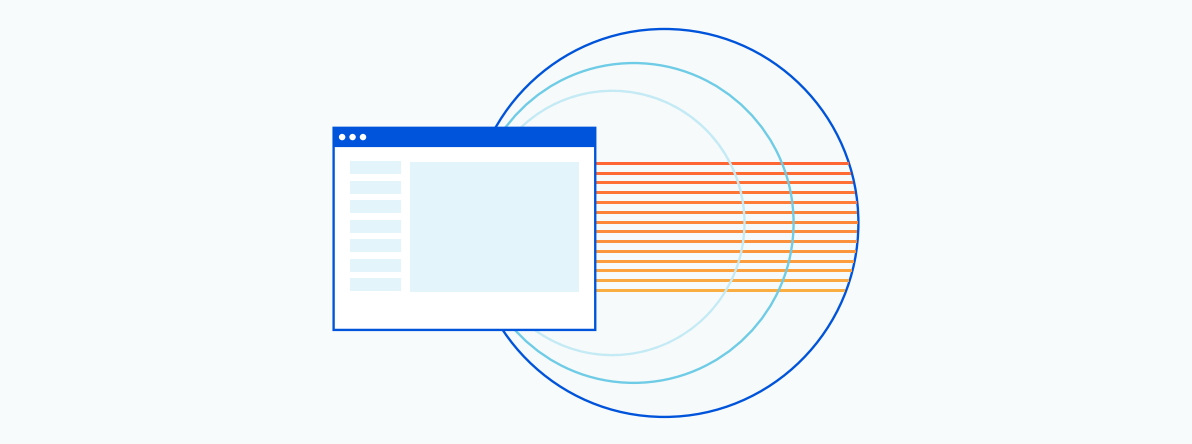
- **On-path attacks:** On-path is a term used to describe an attack that intercepts communication between two devices to manipulate their exchange. Attackers can intercept DNS queries and redirect them to different sites. In some cases, the attack redirects users to a replica of their original destination site. Attackers hope that the replica will fool users into entering their information so that the attacker can steal it. This form of an on-path attack is called DNS spoofing. In other cases, users are redirected to another site entirely that may infect their devices with malware or otherwise attempt to steal user data.
- **DNS tunneling:** In DNS tunneling attacks, attackers use different types of Internet protocols like SSH or HTTP to pass malware into DNS queries.
- **NXDOMAIN attack:** In an NXDOMAIN attack, attackers flood DNS servers to create a denial of service and stop legitimate users from accessing a site.

Without DNS security, businesses are vulnerable to these types of attacks and others, creating a weak link in an overall security strategy. As startups are often working to inspire customer trust, securing customer data by defending against attacks is critical. Fortunately, managed DNS providers can help startups achieve a resilient DNS.

Managed DNS providers like Cloudflare host all DNS records, resolve queries at the edge, and provide integrated DNS Security Extensions (DNSSEC) support. DNSSEC is a security protocol that protects domains from the types of DNS attacks described above. DNSSEC adds a layer of security by adding cryptographic signatures to existing DNS records. The signature ensures that the data is valid and must happen at every stage of the DNS lookup process.

Building a resilient DNS is crucial because almost all Internet traffic requires DNS queries. Additionally, an unsecured DNS leaves user data vulnerable to attacks. Protecting user data is an integral part of an overall security strategy for any company. Because startups do not benefit from a long history that can help create a credible reputation, addressing security gaps like an unsecured DNS is particularly important.

TIP #2



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

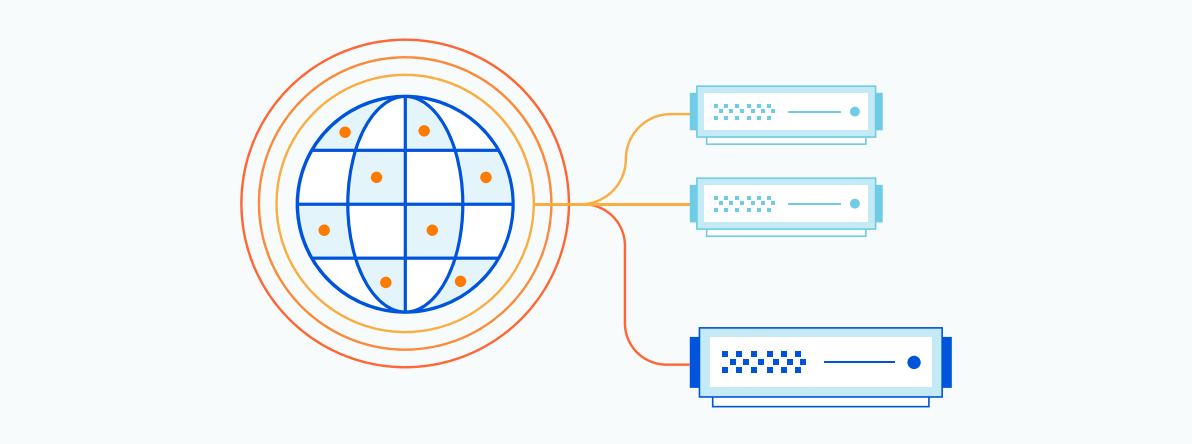
Today, Content Delivery Networks (CDNs) serve most web traffic, including traffic from major sites like Amazon and Facebook. A CDN is a geographically distributed group of servers that speeds up content delivery to globally dispersed users.

With servers in multiple locations around the globe, a CDN distributes content closer to website visitors, and in doing so, reduces network latency and improves page load times. CDNs also cache content — meaning they store and serve static assets across their network. Caching content reduces the number of requests made to hosted web servers and results in lower bandwidth and hosting costs.

CDNs help create a positive online experience because they optimize how quickly users receive content. While all businesses can benefit from a CDN, startups generally have fewer resources, creating pressure to maximize return on investment wherever possible. CDNs are an ideal investment for online performance because they increase page load times while reducing bandwidth costs.

The most effective CDNs have extensive networks. The larger the network, the closer content is distributed to visitors. Other factors to consider when choosing a CDN provider are pricing predictability and the level of visibility they offer into their cache. A CDN provider that offers predictable pricing will ensure that an attack or a traffic surge does not leave your organization with an unexpectedly high bill. Additionally, a CDN that provides greater visibility into analytics equips administrators with the data they need to optimize content caching and further drive down bandwidth costs.

TIP #3



Minimize the risk of site outages by globally load balancing traffic

Maximizing server resources and efficiency is a delicate balancing act. Overloaded or geographically distant servers can increase latency or cause server failure. Poor server performance can result in lost revenue, broken customer trust, and brand degradation.

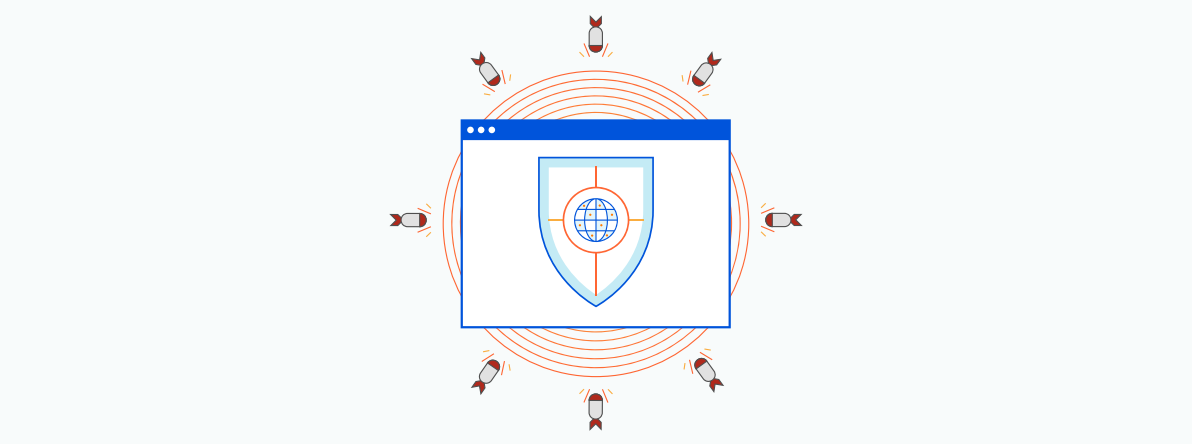
Cloud-based load balancers help optimize server efficiency by distributing requests across multiple servers. Spreading traffic across various servers increases overall capacity, which speeds up load time as requests are processed faster. With cloud-based load balancers, the load balancing decision occurs at the network edge for optimum speed.

Cloud-based load balancers allow 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, so businesses can identify underperforming servers and take preemptive measures before a breakdown occurs.

When selecting a cloud-based load balancer, look for a provider that offers fast failover. Failover is the process of redirecting traffic away from an unhealthy server to a healthy one. The faster a load balancer fails over, the less downtime a site experiences, and the better the user experience.

Load balancing traffic is an essential part of creating a positive online experience because it helps prevent server failure and speeds up load times. The right load balancer can also help ensure that a site or application remains available during a traffic spike. Preparing for traffic spikes is critical for startups, who may experience unpredictable traffic patterns as their business grows.

TIP #4



Protect web applications from malicious attacks

The Internet exposes web-based businesses to a vast spectrum of attacks. While attacks can debilitate firms of any size, startups generally have to work harder to earn customer trust, which puts their brand reputation in a more precarious position. Securing website and customer data is therefore vital for any startup's long-term success. 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. A WAF can protect startups 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. These attacks 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 defend an application 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.

B. DDoS attack protection

A distributed denial of service (DDoS) attack is a malicious attempt to overburden servers, devices, networks, or surrounding infrastructure with a flood of illegitimate Internet traffic. These attacks cause significant service disruptions and prevent customers from making purchases or accessing a business' resources.

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 create latency that can adversely affect a business.

Scrubbing requires re-routing network traffic to centralized servers that filter or 'scrub' out malicious traffic. Re-routing all traffic to a geographically distant scrubbing center takes time, creating significant latency.

Another DDoS mitigation technique uses on-premise hardware boxes to scan traffic and filter out malicious requests. Like scrubbing, the scanning hardware introduces network latency by re-routing network traffic through the boxes to complete the scanning process.

The best way to protect your network from a DDoS attack is to invest in a DDoS mitigation solution that does not scrub data or rely on hardware boxes. Seek providers with expansive networks and high capacity servers because these factors equip them to protect Internet properties from large-scale DDoS attacks. The fastest-working DDoS solutions sit on top of strong networks that allow them to mitigate attacks at the edge. Additionally, because DDoS attacks use traffic volume to overwhelm a network, a powerful mitigation solution absorbs a large amount of traffic to protect Internet properties.

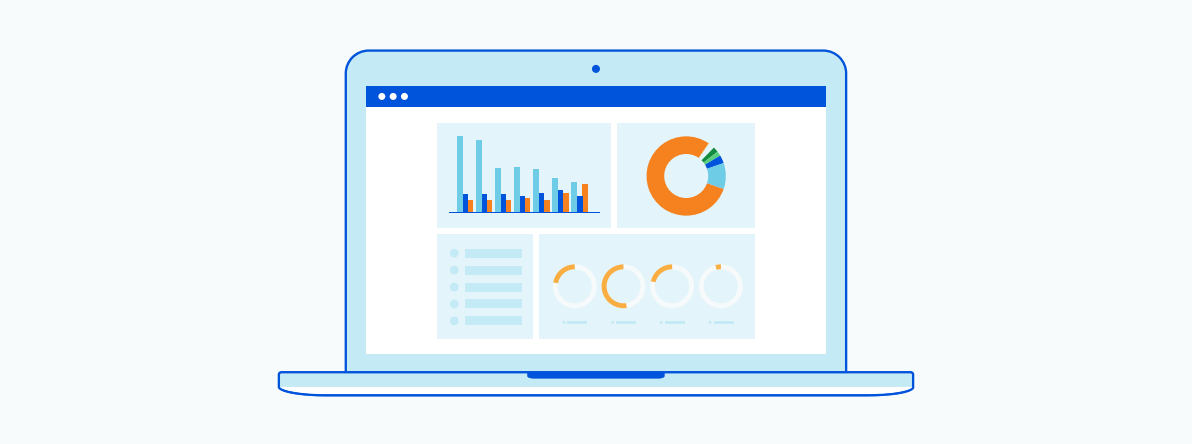
C. Malicious bot mitigation

Sites and applications may become compromised when targeted by malicious bot activity. Malicious bots often take the form of botnets — or networks of infected devices working in tandem — that carry out different types of attacks. Common malicious bot activities include:

- **Credential stuffing:** In credential stuffing, an attacker leverages stolen account credentials — often from a data breach or an otherwise illegal purchase — in an attempt to gain access to an account. Attackers rely on the fact that many people reuse passwords and use stolen account information for one platform, such as a game, to access more lucrative accounts, like bank accounts. Attackers use bots to automate these login attempts in the hopes of accessing more accounts in a shorter amount of time.
- **Content scraping:** Bots can 'scrape' or download and duplicate content from a site. Attackers scrape content to grow their site's organic traffic or otherwise capitalize off the Search Engine Optimization (SEO) value of another site. Content scraping attacks redirect some organic traffic away from the victim's site and degrades the original content's value.
- **Click fraud:** Attackers can also program bots to carry out click fraud. With click fraud, bots engage with a website, app, or ad as though they were a legitimate visitor. Depending on where click fraud takes place, it can have different goals. For example, an attacker might use ad-based click fraud to drive up their victim's advertising budget with illegitimate traffic.

Malicious bots can overwhelm web servers, skew analytics, prevent users from accessing webpages, steal user data, and compromise critical business functions. By implementing a bot management solution, businesses can distinguish between useful and harmful bot activity and prevent malicious behavior from impacting the user experience.

TIP #5



Keep an eye on your analytics

While startups figure out what works best for their business, they often pivot, whether that means making adjustments to their market positioning or their technical infrastructure. Data is crucial to the informed decision-making needed to make these pivots successful. Unfortunately, one of the challenges associated with multicloud or hybrid deployments is a lack of visibility into data across the network. Without network data, businesses may miss opportunities to improve performance or address trends in security threats.

A security and performance provider with a robust analytics offering supplies businesses with data about everything from server health to cache hit ratio. The cache hit ratio describes how effective a cache is at fulfilling content requests. Insights like these empower administrators to make optimizations that reduce downtime and drive down bandwidth costs.

TIP #6

Seek an integrated provider

Many organizations find themselves working with multiple providers to meet their security, performance, and reliability needs. However, managing multiple point solutions can present challenges that exacerbate the pressure of dealing with limited time and resources most startups already have. First, stringing together different providers introduces unnecessary complexity because teams will need to learn how to navigate and manage multiple solutions. This complexity also often presents unnecessary expense as companies manage numerous contracts and are likely unable to utilize tools fully.

Working with multiple providers also creates data silos that can lead to security gaps. For example, a web application firewall (WAF) and DDoS mitigation solution may defend Internet properties against separate and distinct attacks. However, an integrated provider will leverage comprehensive network data to better protect an Internet property against both of these attacks.

Choosing a combination of best-in-class point solutions is tempting. However, a combination of point solutions misses out on the intelligence that comes with a layered approach, on top of burdening teams with the need to manage several individual tools.

For startups, reducing complexity wherever possible alleviates pressure on technical team members and creates space for focusing on revenue generation. Moreover, integrated solutions benefit from the intelligence of layering products. This comprehensive intelligence helps startups address security gaps that can leave them vulnerable to costly security breaches. The ease of use that comes with integrated solutions also helps startups save time and effort to focus on growing their business.

Conclusion

To create superior online experiences, startups need to accelerate content delivery and ensure network reliability and protect their web properties from site outages, data theft, and other critical attacks. For startups, in particular, it is essential to choose providers that improve efficiency and reduce complexity. Integrated solutions backed by strong networks empower startups to protect and accelerate their Internet properties without compromising their growth goals.

Backed by a network that spans more than 200 cities in over 100 countries worldwide, Cloudflare provides a scalable, integrated global cloud platform that helps startups 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.