WHITE PAPER

CLOUDFLARE

Five best practices for mitigating DDoS attacks

How to defend against rapidly evolving distributed denial-of-service threats and address vulnerabilities at every layer

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

INDEX

Executive summary

Distributed denial-of-service (DDoS) attacks remain one of the most effective methods cyber criminals use to cause significant financial, operational, and reputational damage to businesses worldwide. Though these attacks take different forms, the goal is always to incapacitate targeted servers, services, or networks by flooding them with traffic from compromised devices or networks.

As organizations harden their defenses, cyber criminals respond with new attack types and higher-capacity attacks. Some of these attacks target layers 3 and 4 of the Open Systems Interconnection (OSI) model in new ways, resulting in network traffic spikes that can exceed 1 terabit per second (Tbps). Others are low-speed, low-intensity layer 7-based attacks designed to fly under the radar and target one or more service gateways and application layers.

Meeting the challenges associated with DDoS attacks requires a comprehensive approach which addresses all threats at all layers. But enhanced security should not come at the expense of performance. While on-premise tools can be part of the answer, a more robust solution will integrate performance with scalable, cloud-based mitigation that works at the network edge to deliver maximum agility and unlimited capacity.

PART 1

What is a DDoS attack?

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt or knock a targeted server, application, or network offline by overwhelming it with a flood of Internet traffic.

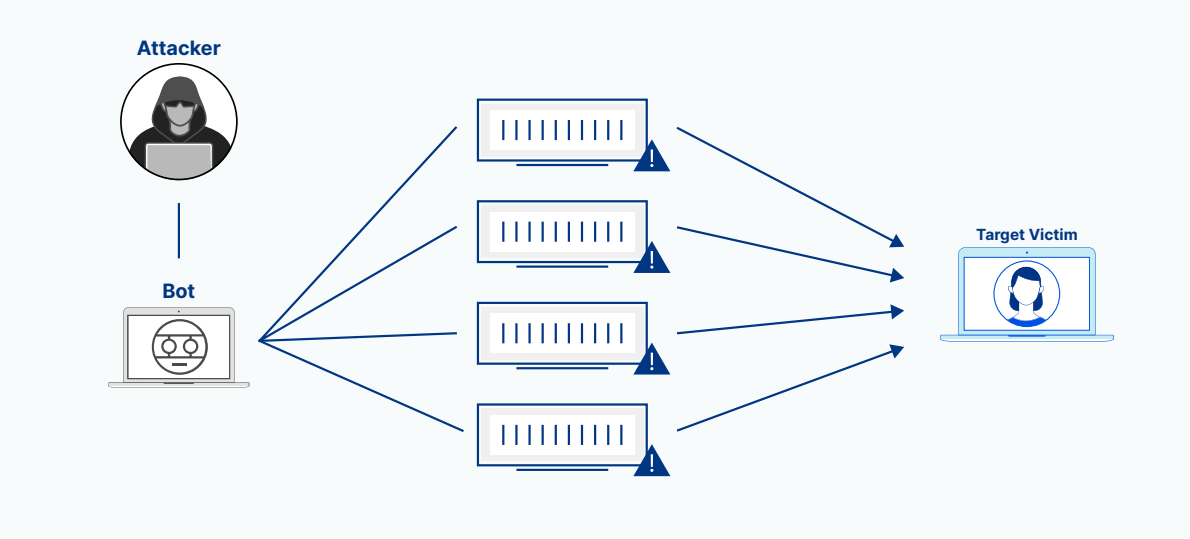
DDoS attackers use malware to take control of online computers, routers, IoT appliances, and other devices, and use them as sources of attack traffic. An infected device is often referred to as a bot, and a group of them is called a "botnet." During the attack, each device in the botnet sends simultaneous requests to the target with the intention of exceeding its traffic capacity limits, resulting in a denial-of-service to normal traffic.

Varieties of DDoS attacks

DDoS attacks can target any of the seven “layers” within the OSI model. While all of these attacks involve inundating targets with malicious traffic, they can be divided into three distinct categories. These categories describe where or how the attacks take place.

Volumetric attacks

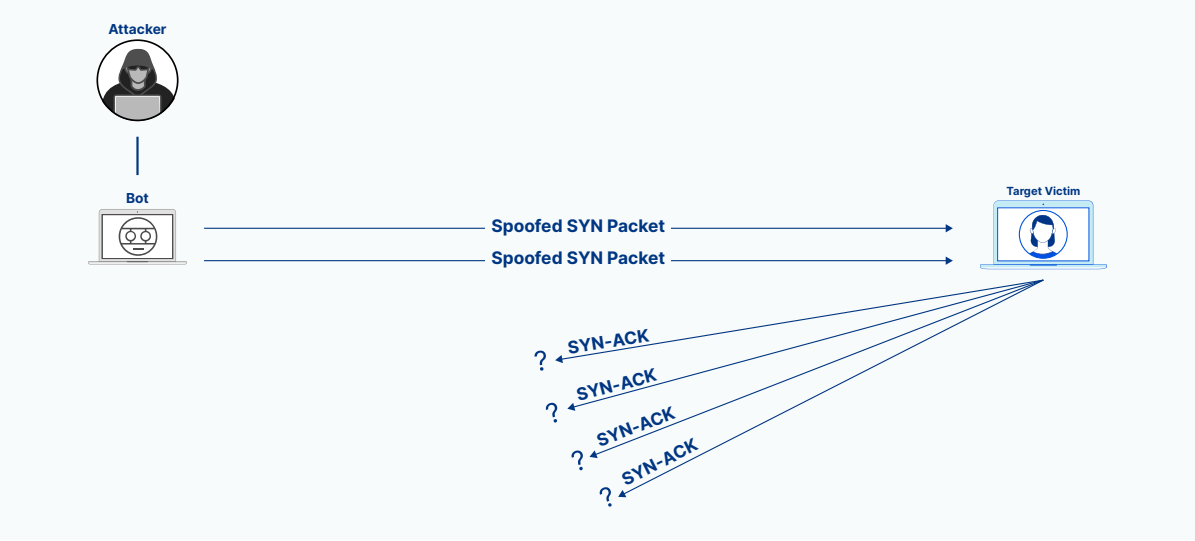
These attacks inundate target sites and networks with huge amounts of traffic — far more so than any other type of attack. These attacks often employ DNS amplification and other brute-force techniques to create massive traffic surges measured in bits per second (Bps). (In DNS amplification, attackers use open DNS resolvers to overwhelm their target with an escalated amount of traffic.)



Protocol attacks

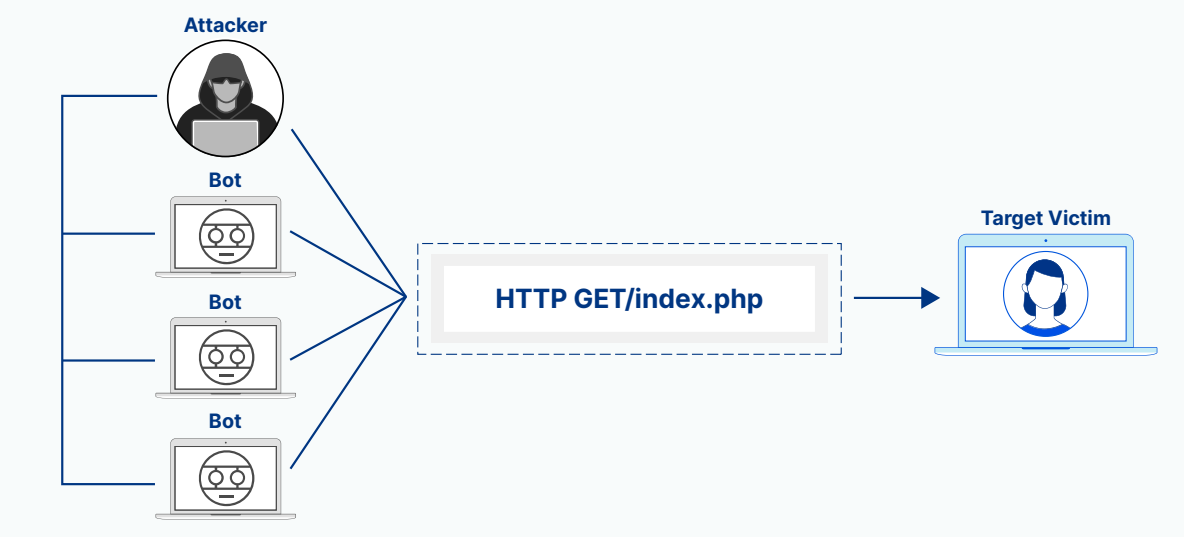
Protocol attacks target vulnerabilities in layers 3 (network) and 4 (transport) of the OSI model and consume all the available capacity of web servers or their intermediate resources — including firewalls and load balancers. These attacks are all measured in packets per second (Pps) and can include:

- SYN floods: This attack involves repeatedly sending initial connection request (SYN) packets to overwhelm all available ports on the targeted server.
- Ping of Death attacks: Attackers send the target a packet exceeding the maximum allowable size, causing it to freeze or crash.
- Smurf DDoS: In this attack, threat actors flood servers with Internet Control Message Protocol (ICMP) packets.



Application layer attacks

These attacks target OSI layer 7, where webpages are generated on the server and delivered in response to HTTP or HTTPS requests. These attacks are similar to repeatedly refreshing webpages on many different computers simultaneously. Thus, the resulting flood of HTTP/S requests is measured in requests per second (Rps).



There is some overlap between these types of attacks. Some protocol attacks can be volumetric, for instance. Then there are multi-vector attacks, in which attackers target multiple layers of the protocol stack — either at the same time, or in response to the target's countermeasures.

The impact of DDoS attacks

The immediate impact of a successful DDoS attack is reduced performance or an outright outage for the targeted service. Some or all parts of the service may be inaccessible altogether.

These performance challenges have broader effects. For web applications, poor performance has a number of negative consequences, including higher bounce rates, lower conversions, and a tarnished brand reputation. For corporate networks, poor performance keeps employees from accomplishing many day-to-day tasks.

In addition, some DDoS attacks are smokescreens for other attacks, keeping security teams distracted while the attacker pursues their ultimate goal through another vector. In such circumstances, the targeted organization could suffer unwanted application access, malware infection, data loss, or worse.

PART 2

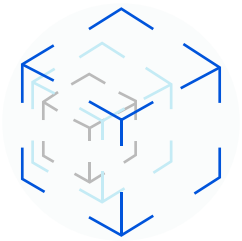
Emerging trends in DDoS attacks

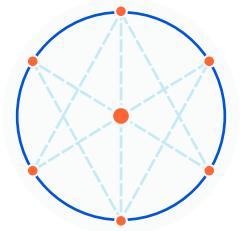
Generally speaking, companies need a few core capabilities to protect themselves against DDoS attacks:

- Differentiate between attack traffic and legitimate traffic
- Detect bad bots and block malicious bot traffic without interrupting legitimate user traffic
- Analyze traffic to find malicious patterns that can aid in improving defenses

However, some emerging trends are making DDoS security more challenging.

PART 2 — EMERGING TRENDS IN DDOS ATTACKS





Volumetric attacks persist and are growing larger

Volumetric attacks can easily overwhelm unprotected organizations. It does not help that the size of these attacks only continue to grow.

In November 2021, Cloudflare automatically blocked a record-breaking multi-vector DDoS attack that peaked just below 2 Tbps. The attack, which was the largest Cloudflare has ever observed, was tied to 15,000 bots running a variation of Mirai Botnet code. Unfortunately, attacks associated with the famous Mirai Botnet and variations of its code have recently resurfaced.

For example, in the summer of 2021, another Mirai-variant botnet launched UDP- and TCP-based attacks that surpassed 1 Tbps multiple times, peaking at approximately 1.2 Tbps.

Outside of Mirai-related attacks, Cloudflare network data demonstrates that the majority of attacks remain under 500 Mbps. That said, in Q3 of 2021, attacks between 500 Mbps and 1 Gbps increased by 289% quarter over quarter (QoQ) while those ranging from 1 Gbps to 100 Gbps grew by 126%.

Network bandwidth can vary greatly depending on an organization's size and the applications they use, meaning some organizations can be easily knocked offline by relatively small attacks if they are unprotected. So as volumetric attacks grow in size, companies should evaluate the capacity of their DDoS mitigation solution.

Attacks are increasing in complexity

The prevalence of multi-vector attacks reflects growing complexity in DDoS attacks.

An example of a multi-vector attack is the recent surge in attacks against Voice over Internet Protocol (VoIP) providers. VoIP providers specialize in technology for communicating over the Internet using voice, video, etc. These attacks have combined L7 attacks targeting critical HTTP websites and API endpoints with L3/4 attacks targeting VoIP server infrastructure.

In multi-vector attacks, attackers use multiple attack vectors (often dynamically), making it all the more difficult to differentiate between legitimate and malicious traffic. Unfortunately, attempts to drop or limit traffic are of no use if the attack adapts to circumvent this countermeasure.

The emergence of new attack methods — or the rise of previously uncommon methods — is another example of DDoS complexity. For example, Cloudflare found that in Q3 of 2021, DTLS amplification attacks increased by 3,549% from the previous quarter. Similarly, Cloudflare network data showed that amplification DDoS attacks abusing the Quote of the Day (QOTD) protocol increased by 123% QoQ in Q2 2021. In the same quarter, attacks over the QUIC protocol grew 109% QoQ.

With attackers constantly finding new ways to launch more complex attacks, it is crucial for organizations to protect themselves against DDoS attacks at every layer.

PART 2 — EMERGING TRENDS IN DDOS ATTACKS

Ransom DDoS attacks are on the rise

Another important trend is the rise of ransom DDoS attacks. In a ransom DDoS attack, an attacker will threaten an organization with a DDoS attack in exchange for a ransom sum. In some cases, the attacker will launch a small DDoS attack to prove they are able to and will follow through on the threat. Ransoms are commonly requested in Bitcoin or other forms of cryptocurrency.

In the first half of 2021, 11% of surveyed Cloudflare customers who were targeted by a DDoS attack said the attacker sent a threat or ransom letter beforehand.

For example, Cloudflare onboarded a Fortune 500 company to Cloudflare Magic Transit (which provides DDoS protection and more for on-premise networks) in 2020. The company had received a ransom letter from a cyber criminal group demanding 20 Bitcoin. To prove their intentions, the group had already launched Gb-strong attacks at a single server.

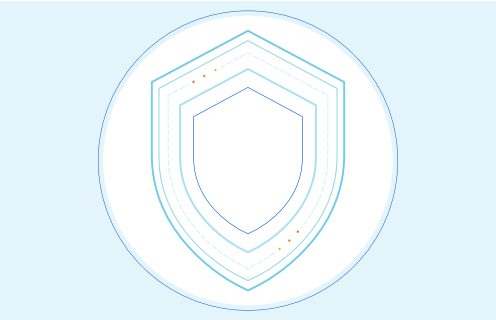
Based on these requirements and evolving trends, here are five DDoS mitigation practices for organizations to prioritize.

PART 3

Best practices for DDoS mitigation

- Bolster protection tactics
- Prioritize the two most important metrics — capacity and time-to-mitigation
- Consider always-on vs. on-demand protection
- Never sacrifice performance for security
- Embrace threat intelligence to stay ahead of attackers

1. Bolster protection tactics



Because DDoS attacks can happen at multiple layers of the OSI stack, it is important to embrace comprehensive protection. However, traditional DDoS solutions are not the only way to go about this. The following tactics can supplement a DDoS solution and protect servers and networks.

Protect servers with a reverse proxy

If your objective is to protect web servers, a reverse proxy will prevent attackers from being able to identify and target your servers' IP addresses. Instead, they will only be able to target the reverse proxy, thereby protecting your servers.

Some companies build or deploy their own reverse proxies, but this requires intensive software and engineering resources, as well as significant investment in physical hardware.

One of the easiest and most cost-effective ways to realize the benefits of a reverse proxy is to use a content delivery network (CDN). CDNs are distributed networks of proxy servers that reduce latency by caching (or storing copies of) content closer to end users.

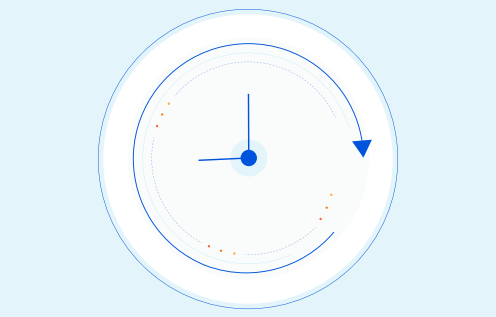
Look for a CDN with global server load balancing, so that your site can be distributed on several servers around the globe. This way, DDoS attacks will be mitigated closer to the source without impacting performance. (See Tip 4 for more on security and performance tradeoffs.)

Protecting networks

If the goal is to protect network infrastructure, Border Gateway Protocol (BGP) rerouting can be used to redirect traffic to scrubbing centers where malicious traffic can be filtered out. That said, rerouting all traffic to a limited number of geographically distant scrubbing centers can add considerable latency.

For this reason, cloud-based DDoS mitigation solutions of sufficient scale are recommended. With cloud-based mitigation, autonomous system numbers (ASNs) are advertised by the mitigation provider, so traffic is routed direct-to-scrub instead of going to the origin server. In this setup, traffic is filtered closer to the source of the attack, further reducing latency.

2. Prioritize the two most important metrics — capacity and time-to-mitigation



The most important factors in DDoS protection are the strength of protection (capacity) and how quickly it works to neutralize attacks (time-to-mitigation).

Capacity

The traditional approach to absorbing spikes in traffic generated by DDoS attacks has been to invest in on-premise hardware. But this quickly becomes expensive, as companies must pay for capacity they have specifically purchased for isolated attacks and are thus not often using. Moreover, even the most robust enterprise-grade infrastructure may be overwhelmed by the largest volumetric attacks.

Rate limiting, or restricting the amount of requests a server will accept during a time period, can help. However, rate limiting alone slows down performance during spikes of legitimate traffic, and cannot withstand more complex attacks.

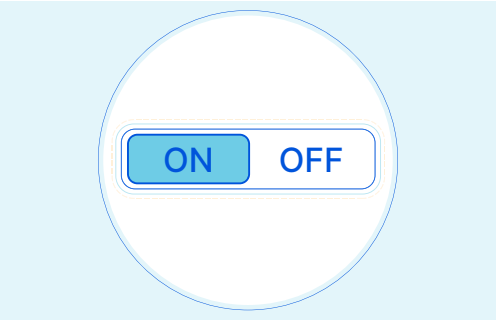
Thus, it is important to prioritize high-capacity solutions. Cloud-based DDoS mitigation with resources that scale can absorb even the largest of attacks, leaving your organization unscathed.

Time-to-mitigation

When even a few moments of reduced availability can lead to significant lost revenue and productivity, time-to-mitigation (TTM) becomes paramount. To reduce TTM, you will need to ensure traffic can failover to an alternate site in the event of an outage—but that will only work for so long before your infrastructure is overwhelmed.

By contrast, cloud-based DDoS protection at the edge helps reduce TTM because attacks are mitigated near the source.

3. Consider always-on vs. on-demand protection



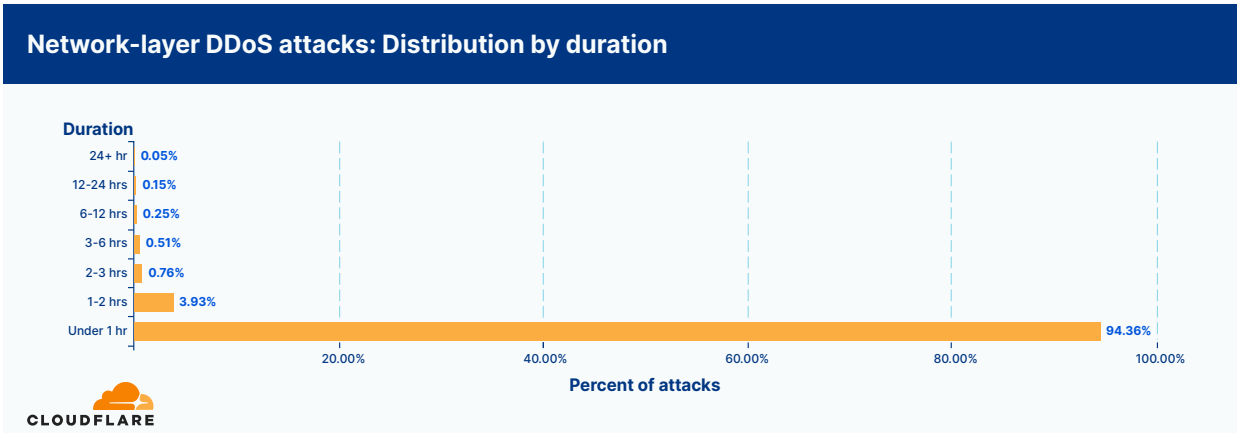
With on-demand mitigation services, traffic flows as it normally does until a potential DDoS attack is detected. At that point, traffic is re-routed to the cloud mitigation service, filtered, and passed back to the server of origin.

You only pay for DDoS mitigation when it is needed, and no management or additional resources are required. But there are tradeoffs, specifically around TTM. Stopping the attack takes longer because traffic spikes must reach certain thresholds before analysis begins and someone manually turns on the mitigation service.

On-demand solutions do not stand up well against short-lived attacks, which Cloudflare network data shows the majority of attacks are. For example, in Q3 2021, over 94% of network-layer attacks lasted under an hour. Short-lived attacks may not sound intimidating, but if on-demand protection is not turned on in time, they can have a major impact. Not to mention, even a few minutes of downtime can be detrimental under certain circumstances.

Attackers may also employ these attacks to test an organization's defenses before launching a larger attack.

In contrast, always-on mitigation continuously routes and filters all site traffic. This way, only clean traffic reaches the customer's servers. While more expensive than on-demand services, always-on mitigation provides uninterrupted protection. This reduces TTM, because the service never needs to be turned on manually.



Source: https://radar.cloudflare.com/notebooks/ddos-2021-q3

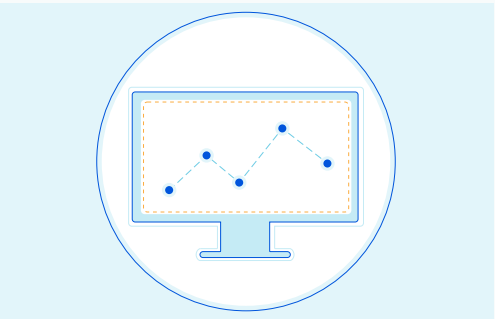
4. Never sacrifice performance for security

Today's digital consumer expects websites and applications to be constantly available and load quickly. In fact, most people will perceive latency at just 100 - 120 milliseconds. But latency is more than an inconvenience, because every additional second of latency reduces conversion rates by 4.42%. Thus, securing against DDoS attacks without diminishing performance requires a careful balancing act.

Many organizations attempt to mitigate this by redirecting traffic to scrubbing centers that filter traffic. However, these scrubbing centers are often far away from the traffic source or the destination network, creating a bottleneck that increases latency. This forces the organization to choose between performance and security.

Edge-based cloud mitigation services offer a solution to this balancing act. Rather than mitigating attacks at centralized data centers, these solutions are built on distributed networks and mitigation runs on every server in the network. This means that detection and mitigation runs as close to the attack source as possible, reducing TTM.

5. Embrace threat intelligence to stay ahead of attackers



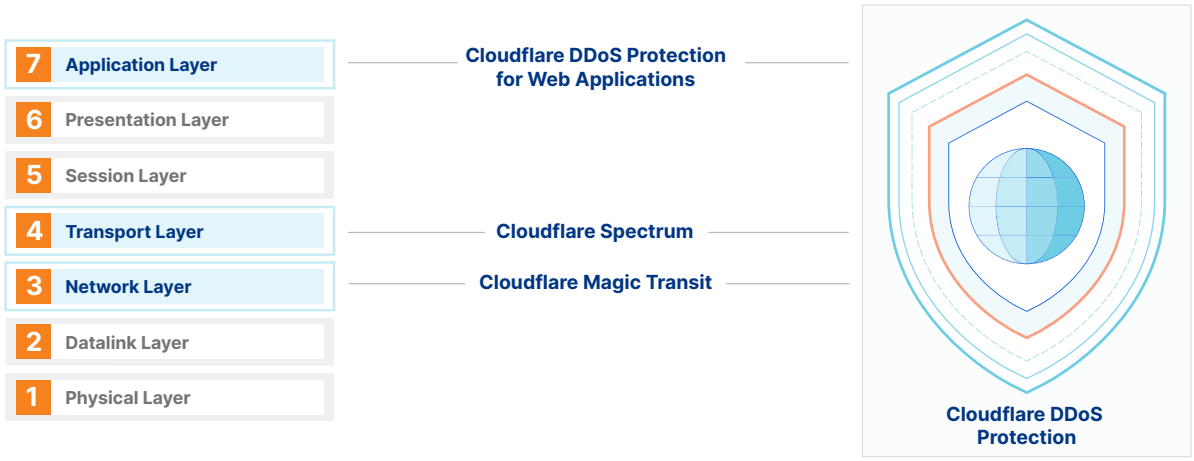
Overcoming increasingly complex DDoS attacks requires more than just a layered approach. It requires you to continuously analyze traffic for malicious patterns that can help you develop the intelligent, adaptive defenses you need to fend off future attacks.

Cloud-based DDoS mitigation systems often employ machine learning to detect and mitigate emerging attacks before they happen. This is called threat intelligence. When evaluating cloud-based mitigation services, it is important to look beyond capacity or transfer and filtering speeds, and consider network intelligence. The larger and more robust the mitigation network, the richer the intelligence it can provide on evolving attack patterns—and the more proactive protection will become.

How Cloudflare can help

The Cloudflare layered security approach combines multiple DDoS mitigation capabilities into one service that prevents disruptions caused by malicious traffic while allowing clean traffic through. We keep websites, applications, APIs, and entire networks up and running with high availability and performance.

With data centers in more than 250 cities in over 100 countries, and over 100 Tbps of network capacity, Cloudflare mitigates DDoS attacks close to the source.



Fast, automated mitigation

Unlike traditional solutions that depend on scrubbing centers, Cloudflare hosts security services on every server in our network to protect against DDoS attacks of any size or complexity.

Comprehensive protection

Cloudflare DDoS mitigation detects and blocks layer 3, 4, and 7 attacks at the network edge. Plus, Cloudflare Spectrum proxies traffic through Cloudflare data centers and protects TCP/UDP applications.

Threat intelligence at global scale

Cloudflare DDoS protection is fueled by the intelligence of our global network, which protects millions of Internet properties. This intelligence allows us to identify anomalous traffic and protect against sophisticated and emerging attacks.

Cost-effective protection

All Cloudflare plans offer unlimited and unmetered mitigation of DDoS attacks, regardless of size, at no extra cost — and no penalty for attack-related traffic spikes.

PART 3 - BEST PRACTICES FOR DDOS MITIGATION

Ease of use and management

Our always-on, cloud-based DDoS protection is built on an intuitive interface that empowers users to quickly and easily protect their Internet properties against DDoS attacks of any size or complexity in just a few clicks.

Integrated security and performance

Our protection is designed to integrate, learn, and operate seamlessly with other security and performance solutions, including Cloudflare Web Application Firewall, Cloudflare Bot Management, Cloudflare Magic Transit, Cloudflare Load Balancing, Cloudflare CDN, and more.

Data analysis, your way

Cloudflare Analytics enables you to analyze DDoS events through the Cloudflare integrated dashboard or GraphQL. Cloudflare logs can also integrate with leading third-party security information and event management (SIEM) tools.

Conclusion

An effective strategy for meeting the challenges associated with DDoS attacks requires a comprehensive approach that addresses all threats at all layers. While on-premise solutions can be part of the answer, they quickly get expensive. A more robust solution will integrate performance with scalable, cloud-based mitigation that provisions services at the network edge for maximum agility and unlimited capacity, ensuring resilience against DDoS attacks of any size or complexity.