

EBOOK

Deterring downtime: A guide to DDoS defense models



Content

Click to skip to section

- 3** Introduction: DDoS defense in a hybrid work world
- 4** Understanding cloud-based DDoS mitigation approaches
 - 6** Common limitations of cloud scrubbing methods
 - 7** When time is money: how downtime and latency can impact businesses
- 8** Realize the full promise of cloud-based DDoS defense — and protect against outage-driven revenue loss
 - 9** Case study: Fortune Global 500 company targeted by a ransom DDoS attack
- 11** Conclusion
- 12** Sources

Introduction: DDoS defense in a hybrid work world

The average enterprise now uses over 1,400 distinct cloud services¹ — driven by increasing demand for better, faster applications and customer experiences. However, a byproduct of cloud transformation is an expanding attack surface: more digital services equal more “entry points” for attackers to exploit. The attack surface has also expanded with hybrid work (the combination of in-office and remote work) — necessitated by years of a global pandemic.

All of these factors are increasing the pressure on resource-strapped businesses. Not only do IT and security teams need to deliver more resilient applications and networks, they also need to protect users and devices, regardless of location, against evolving threats.

Some of these threats include more frequent, longer, and larger distributed denial-of-service (DDoS) attacks. In February 2023, Cloudflare detected and mitigated the [largest HTTPS DDoS attack](#) (71 Mrps) on record. Our data also shows quarter-over-quarter [increases](#) in hyper-volumetric DDoS attacks (attacks above 100 Gbps) in 2022.

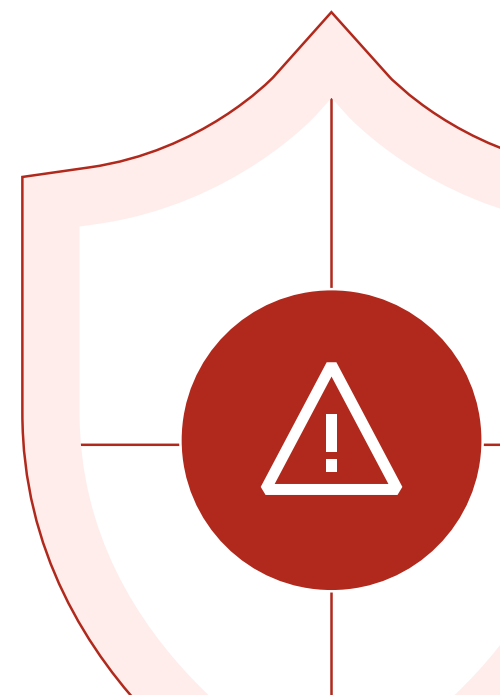
Today’s economic and hybrid work realities require businesses to reevaluate their DDoS defenses: the risk of downtime, data theft, network infiltration, and financial losses are too great.

Research shows that over 60% of outages cost more than \$100,000, and 15% of outages cost more than \$1 million². In one example, downtime due to a series of DDoS attacks cost one company nearly \$12 million³.

These realities make DDoS defense critical for organizations of all sizes. And the manual approaches of the past are no longer enough. While attacks may be initiated by humans, they are executed by bots — and to win, you must fight bots with bots. Detection and mitigation must be automated as much as possible.

This ebook explores:

- Different models of cloud based DDoS protection
- Overcoming the limitations of always-on cloud scrubbing
- How a Fortune Global 500 company thwarted a ransom DDoS attack with Cloudflare

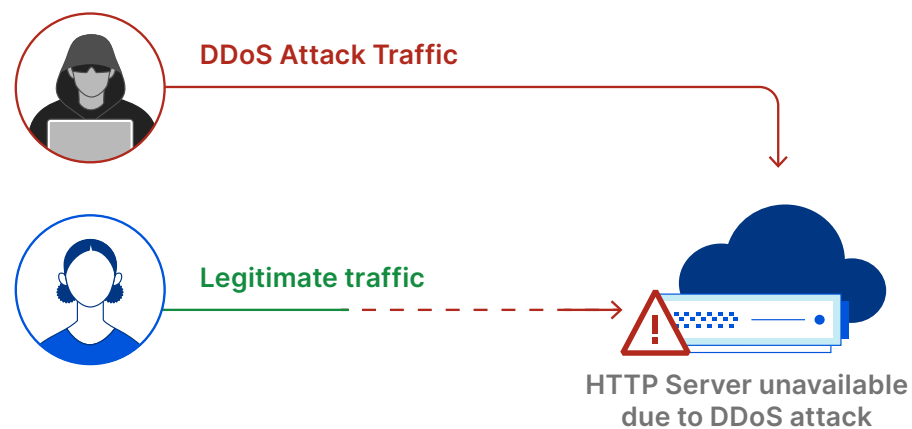


Understanding cloud-based DDoS mitigation approaches

A [DDoS attack](#) is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. An effective DDoS solution will tell you exactly when, where, and how this “traffic jam” is occurring — while absorbing and rerouting malicious traffic so it won’t interfere with legitimate traffic. Highly trafficked destinations, coupled with unprotected Internet properties and networks, are all common targets.

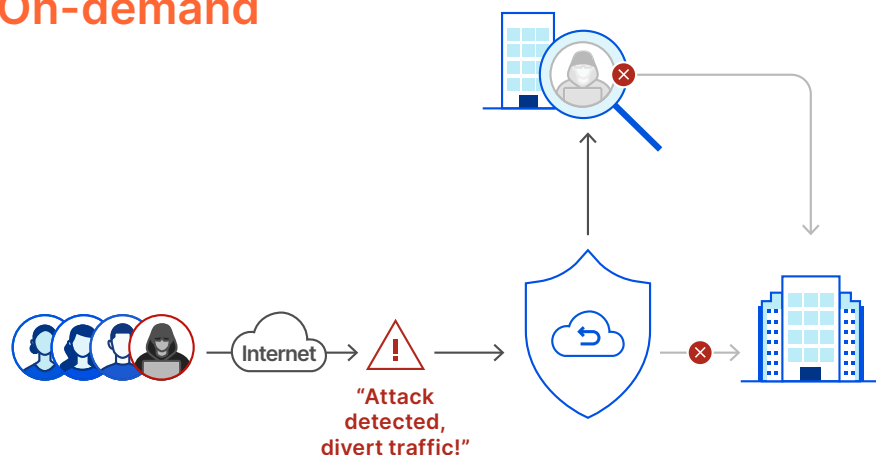
While DDoS attacks are nothing new, new approaches are required to stop them. As applications have migrated to the cloud, the market for on-premises DDoS solutions has also shrunk⁴ — instead, more organizations are turning to the cloud for DDoS protection.

With many varieties of cloud-based protection, a cloud provider sits in front of an organization’s applications and infrastructure and diverts all traffic to a scrubbing center to be ‘cleaned’. Only legitimate traffic is sent back to the customer. This ‘cloud scrubbing’ motion can be activated in two ways: *on-demand* or *always-on*.



A diagram of an application-layer DDoS attack denying service to legitimate users

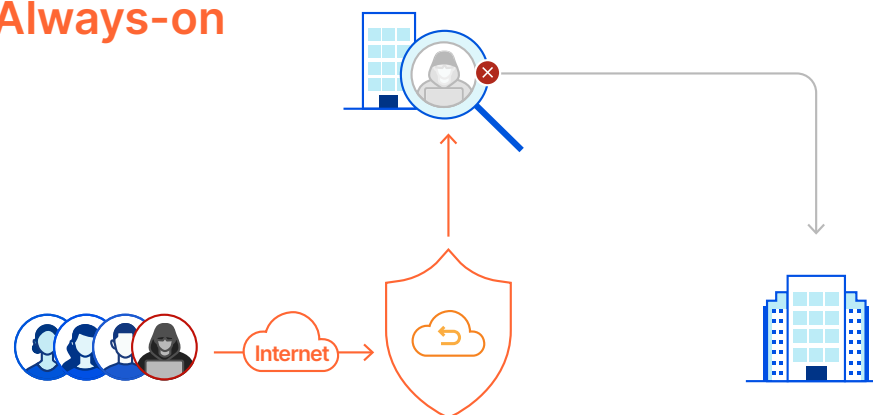
On-demand



During ‘peacetime,’ on-demand cloud scrubbing ensures all traffic reaches applications and infrastructure without any redirection. Traffic only gets diverted to the cloud scrubbing provider in an active DDoS attack situation.

If inbound traffic crosses a pre-configured threshold (e.g., 70% of the link capacity) or if a large attack is detected, then on-demand cloud mitigation mode is activated, and traffic is diverted to the closest scrubbing center for processing.

Always-on



This essentially hands-off approach to cloud scrubbing always routes traffic through your cloud provider’s data center for threat inspection — even during peacetime.

An always-on model helps minimize time from detection to mitigation without any service interruption.



While both on-demand and always-on techniques offer different benefits, they each can present limitations in different circumstances — as described in the next section.

Common limitations of cloud scrubbing methods

On-demand cloud scrubbing challenges

Delayed attack response:

- On-demand requires traffic to be re-routed to the cloud provider in a DDoS attack. It can take several minutes for this switch to take place, in addition to the time it takes to manually respond to the attack (e.g. tell the provider to turn on the service). If on-demand protection is not turned on in time, they can have a major impact.

Increased cost in the long run:

- On-demand cloud providers often charge per byte of attack traffic. While you only pay for what you use, this could end up costing more if your organization experiences more frequent DDoS attacks.

Potential missed attacks:

- DDoS attacks that do not cross the utilization threshold can go undetected, congesting network links that affect legitimate traffic.
- Network links also do not monitor for higher-layer protocol attacks at the SSL and application level.



Always-on cloud scrubbing challenges

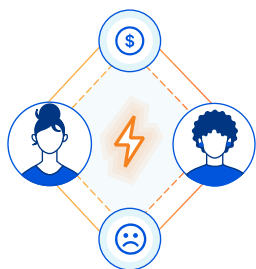
Latency problems leading to negative user experiences:

- Many cloud DDoS mitigation providers have a set of distant data centers dedicated to scrubbing network traffic that are far from where the attack traffic originates. Fewer scrubbing centers generally equate to greater latency. This traffic backhaul can also introduce latency and create noticeable delays.
- Data centers dedicated to DDoS scrubbing inspect also often only the network layer. For functions that live on other layers, such as the web application firewall or content caching, this traffic is typically processed at an alternate data center — adding even more latency.

Higher total cost of ownership:

- Always-on cloud scrubbing solutions with limited network capacity may pass their bandwidth limitations on to customers, in the form of higher pricing. Professional services fees may also be tacked on.

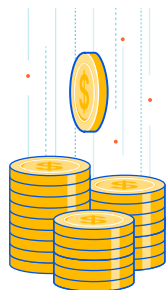
When time is money: how downtime and latency can impact businesses



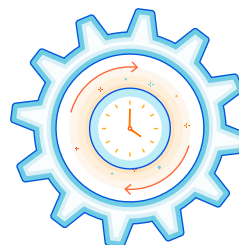
91% of organizations say **hourly downtime costs up to \$300,000** due to lost business, productivity disruptions, and remediation efforts⁵



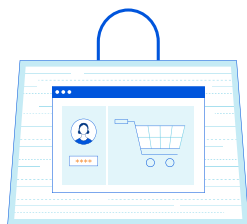
44% of gamers who experience latency respond by **quitting the game they're playing** to try it again later — while **24% will quit to play something else**⁸



For well-known ecommerce companies, downtime can cost up to **\$220,000** per minute⁶



64% of IT decision-makers say the need to deliver a quicker and easier customer experience is a **“significant or major burden on their tech infrastructure”**⁹







90% of shoppers will abandon a site if it doesn't load “in a reasonable time” — and **57% will leave and buy from a similar retailer**⁷

Realize the full promise of cloud-based DDoS defense—and protect against outage-driven revenue loss

Here’s how our unified cloud platform, powered by an intelligent global network, protects against DDoS threats:

On-demand cloud scrubbing relies on human intervention, adding time to the mitigation response. In contrast, always-on cloud DDoS protection is more comprehensive — however, many always-on cloud DDoS vendors rely on distant scrubbing centers that add latency to the user experience.

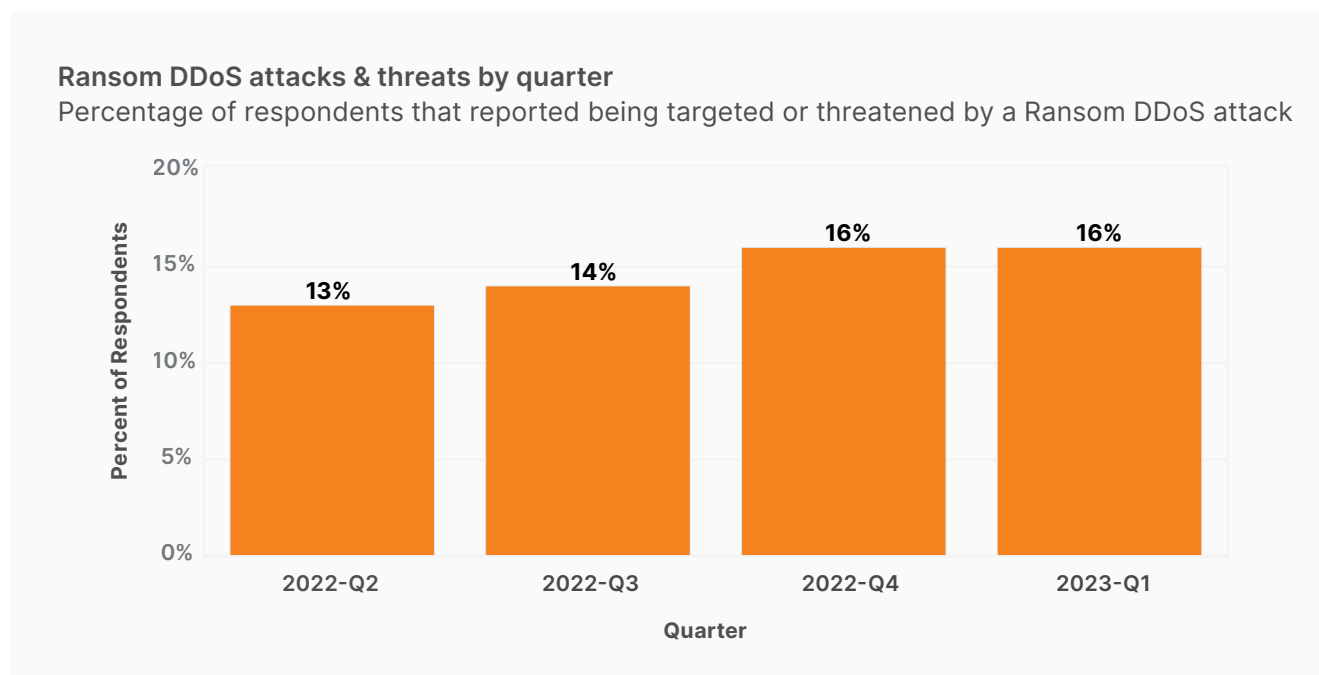
Cloudflare addresses those limitations with a unified security platform — which includes three layers of [DDoS protection](#) (layers 3, 4, and 7) and traffic acceleration for on-premise, cloud-hosted, and hybrid networks. Attack traffic is mitigated close to the source, so your end users have a seamless, performant experience.

 Network-powered security	 Usability, visibility, and self-service	 Threat intelligence at scale	 Industry-recognized DDoS defense
<p>Cloudflare has data centers in more than 285 cities, and a network capacity of 197 Tbps (in contrast, one well-known always-on DDoS mitigation service has fewer than 40 scrubbing centers and 20 Tbps of network capacity).</p> <p>Attacks are automatically absorbed by our network before they ever reach yours, and most malicious traffic is blocked in less than 3 seconds. No backhauling necessary.</p>	<p>Cloudflare DDoS protection is delivered as-a-Service, which means no CapEx investment or hardware lifecycle management required.</p> <p>Plus, it’s self-serviceable with custom configuration capabilities in a single dashboard.</p>	<p>See more, protect more: nearly 20% of the Web runs on Cloudflare. Our customers benefit from the scale and intelligence of our global network, which blocks over 112 billion cyber threats per day.</p> <p>Advanced machine learning models continuously improve our defenses, so we can stay ahead of emerging threats on your behalf.</p>	<p>Cloudflare has been recognized as a Leader in the 2022 GigaOm Radar Report for DDoS Protection. The report evaluated nine different vendors, and Cloudflare was ranked highest overall. Cloudflare was also named a ‘Leader’ in The Forrester Wave™: DDoS Mitigation Solutions, Q1, 2021.</p> <p>Cloudflare received the highest possible scores in 15 criteria, including security operations centers, response automation, performance, and more.</p>

Case study: Fortune Global 500 company targeted by a ransom DDoS attack

A [ransom DDoS](#) (RDDoS) attack, also known as ransom extortion, is when malicious parties attempt to extort money by threatening an individual or organization with a DDoS attack. The number of ransom DDoS attempts steadily increased throughout 2022 — and over 16% of Cloudflare customers received a threat or ransom demand as part of a DDoS attack in Q1 2023.

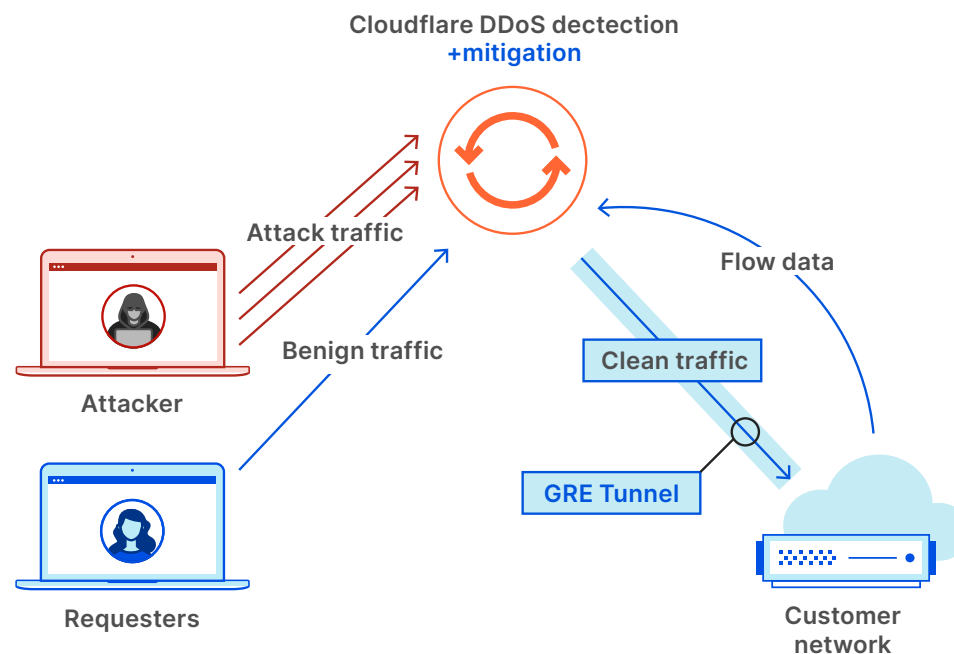
While often confused with ransomware attacks, ransom DDoS attacks work differently and are easier to execute: they don't require tricking the victim into opening an email or clicking a link, nor do they require a network intrusion or a foothold into corporate assets. The increasing availability of [ransomware-as-a-service](#) has also made ransom DDoS a low-effort, low-risk option for attackers.



In late 2020, prior to using Cloudflare for DDoS mitigation, a major Fortune Global 500 company was [targeted](#) by an RDDoS attempt by parties claiming to be the Lazarus Group (a cybercrime group allegedly run by the government of North Korea). The attackers initially sent an email demanding bitcoin and gave them a week to “pay up,” or else a second larger attack would strike, and the ransom would increase.

After receiving the ransom note and noticing a significant increase in traffic towards one of their global data centers, the company contacted their on-demand scrubbing center service. It took them over 30 minutes to activate the vendor’s service and redirect traffic to the scrubbing center. Activating the on-demand service also caused networking failures and resulted in multiple incidents.

Following the initial attack and challenges with their on-demand provider, the company decided to onboard [Cloudflare Magic Transit](#) — Cloudflare’s always-on protection against network layer DDoS attacks. Although the attackers promised a second, huge attack, it never happened.



Cloudflare Magic Transit for DDoS protection at the network layer

“One of the key differentiation is the attack and traffic analytics that we see that our incumbent provider couldn’t provide us. We’re seeing attacks we never knew about being mitigated automatically.”

Incident Response and Forensics Team
Fortune Global 500 company

Conclusion

As DDoS attacks increase in frequency and complexity in the post-pandemic era, it is important to keep legitimate traffic going to help protect your bottom line. With the ability to quickly and effortlessly protect against attacks, without the latency problems or high costs commonly associated with other providers, Cloudflare makes it easy to opt for an always-on cloud strategy.

To learn more about protecting against network DDoS attacks with Cloudflare, [request a demo](#).

To learn more about a single global network with built-in Zero Trust functionality, DDoS mitigation, network firewalling, and traffic acceleration, [click here](#).



Sources

- 1 Langrock, Sam. "The Cloud has Complicated Attack Surface Management." Recorded Future, April 3, 2023, <https://www.recordedfuture.com/the-cloud-has-complicated-attack-surface-management>
- 2 "Uptime Institute's 2022 Outage Analysis Finds Downtime Costs and Consequences Worsening as Industry Efforts to Curb Outage Frequency Fall Short." Uptime Institute, June 8, 2022, <https://uptimeinstitute.com/about-ui/press-releases/2022-outage-analysis-finds-downtime-costs-and-consequences-worsening>
- 3 Cimpanu, Catalin. "Bandwidth.com expects to lose up to \$12M following DDoS extortion attempt." The Record, November 1, 2021, <https://therecord.media/bandwidth-com-expects-to-lose-up-to-12m-following-ddos-extortion-attempt>
- 4 Holmes, David and Blankenship, Joseph, et al. "The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021," Forrester, 3 March 2021
- 5 Didio, Laura. "The Cost of Enterprise Downtime," TechChannel, September 30, 2021. <https://techchannel.com/IT-Stratgy/09/2021/cost-enterprise-downtime>
- 6 "The Cost of Downtime for the Top US Ecommerce Sites," Gremlin, accessed May 8, 2023, <https://www.gremlin.com/ecommerce-cost-of-downtime>
- 7 Crets, Stephanie. "Most consumers abandon a slow-loading ecommerce site." DigitalCommerce360, August 21, 2020. <https://www.digitalcommerce360.com/2020/08/21/most-consumers-abandon-a-slow-loading-ecommerce-site>
- 8 Duperre, Mathieu. "44 percent of gamers respond to latency by quitting their games — what can we do to stop this?" PocketGamer.biz, October 24, 2022, <https://www.pocketgamer.biz/asia/comment-and-opinion/79974/44-per-cent-of-gamers-respond-to-latency-by-quitting-their-games-what-can-we-do-to-stop-this>
- 9 "Infinity Data and the battle to conquer latency." Hazelcast and Intel, November 2019. <https://hazelcast.com/resources/infinity-data-report>