



5 Questions to Ask When Choosing a DDoS Protection Vendor



The figures vary, but experts agree that cybercrimes, including DDoS attacks, have been increasing in scale and frequency since the start of the pandemic. One figure speculates that DDoS attacks alone increased by 341% during the first year of the pandemic.¹

With more people than ever working from home, the average business's network is far more distributed than ever before in a time when people rely on the Internet more than ever. As a result, today's cyberthreat landscape has become extremely complex and cybercriminals are finding smarter ways to attack the systems we all rely on.

DDoS attacks are just one of the ways cybercriminals are halting business and hurting organizations. Simply put, DDoS attackers operate by sending large quantities of traffic to a target system using a network of "botnets" or malware-infected Internet-connected devices. The goal of these attacks is to take the target's website or network offline for a period of time, rendering their service unavailable.

Today's attackers can take down entire websites in this way for as little as \$10.² In contrast, DDoS attacks cost a business an average of \$30,000 hourly.³ With billions of Internet-connected devices around today, amassing a botnet army with the capability to take down websites is accessible to even the most entry-level cybercriminal.

Before equipping your business with the right solution, it's important to understand what your risk is, what kinds of attacks you should protect against, the DDoS protection options available, and what it will cost you.

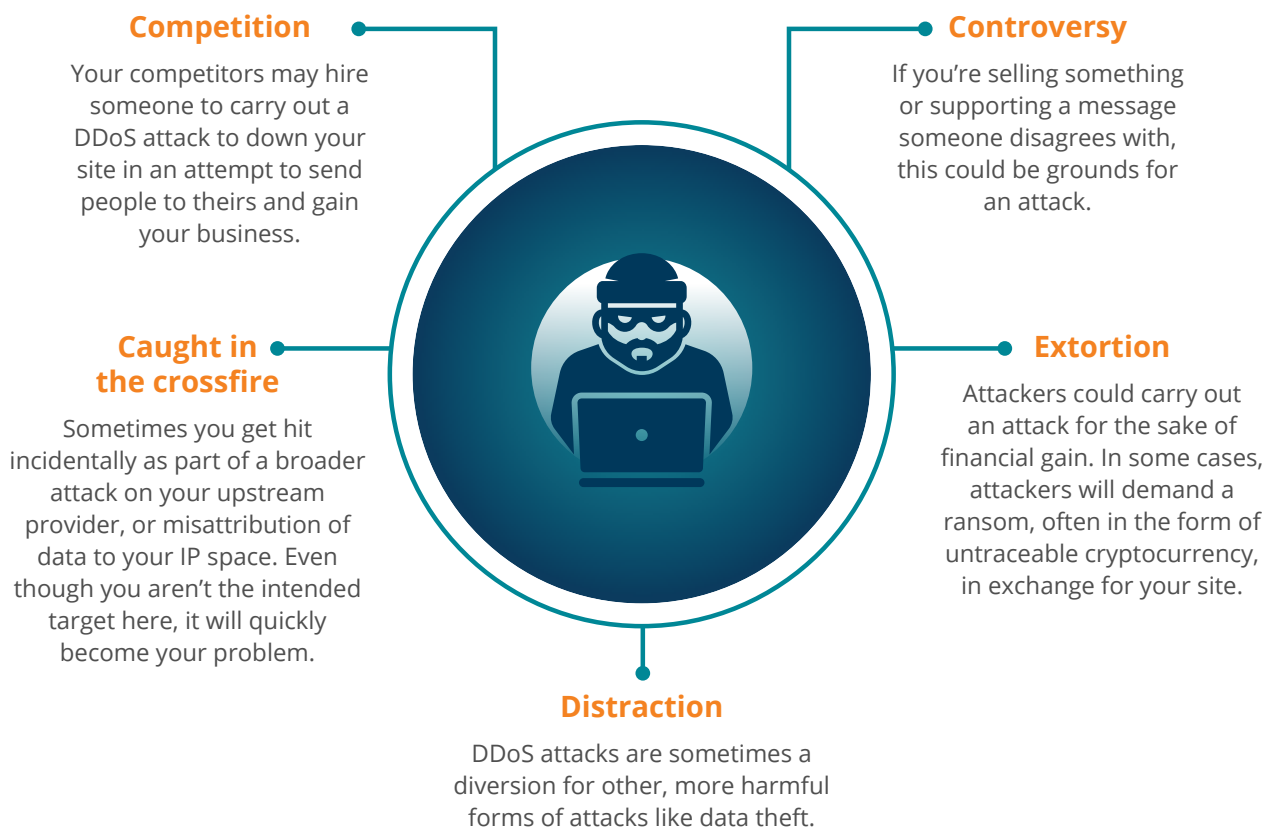
This guide will take you through the five questions to ask before purchasing DDoS protection.

**Any company
in any industry
can become
the victim of a
DDoS attack.**

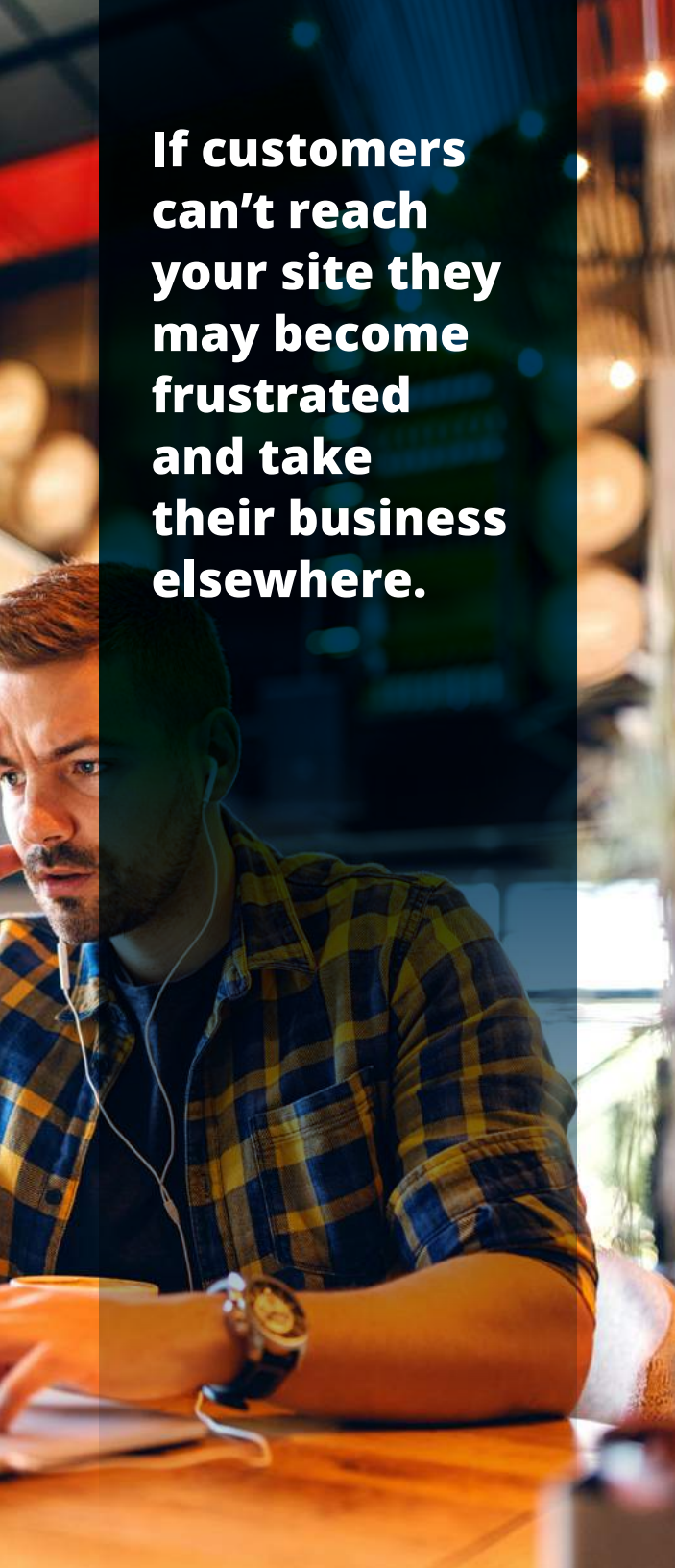
1. Could my business become the target of a DDoS attack?

The simple answer is, if your business is online, you could become the target of a DDoS attack. Companies across industries are finding themselves the target of DDoS attacks.

The reasons for carrying out these kinds of attacks vary. Here are a few reasons why you might find your business the victim of a DDoS attack:



In short, there are a lot of reasons that you could become a victim of a DDoS attack. The reason you're a target may even be no reason at all. It's important to consider yourself at risk of this common form of attack, even if you don't think there's a reason you'd be targeted.



**If customers
can't reach
your site they
may become
frustrated
and take
their business
elsewhere.**

2. What's at risk if my business falls victim to an attack?

There are four main ways a DDoS attack can impact your business.



1. Disrupted business continuity

If your website is down, legitimate traffic from potential customers won't be able to reach you. If your business relies on your website to operate, DDoS attacks can have a serious negative impact. What's more, restoring your site will take time and money. Day-to-day operations could take hours to get back up and running.



2. Financial and business loss

Most obviously, you can lose money from lost business. In the short term, if customers can't reach your site they may become frustrated and take their business elsewhere. It's possible that you could lose these customers for good. One study found that 88% of online customers won't return to a website after a bad experience.⁴

What's more, DDoS attacks can impact your site's search engine rankings. This makes it more difficult for legitimate users to find you on search engines.

Secondly, if you find your business the victim of a ransom DDoS attack, you may be paying even more to get your site back up.



3. Damaged reputation

Needless to say, falling victim to any kind of cybercrime doesn't fare well for your business's reputation. Not only may customers find themselves frustrated with a downed website, they also may question if they can trust you with their data. Although data theft is not the goal of DDoS attacks, these attacks call into question your security level as a whole.



4. Vulnerability to a bigger attack

If you're pooling your resources to handle a DDoS attack, you may find your business vulnerable to another style of cyberattack. It's important to always remain vigilant and keep an eye out for strange activity across the network, especially in the wake of an attack.



**It's important
to protect your
network in a
holistic way.**

3. What kind of DDoS attack could my business be targeted with?

Your website certainly needs protection, but protecting your web presence is only step one. Less visible systems that are accessed via the public Internet like your phones, VPN remote access, and door access controls can also fall victim to attacks. DDoS attacks can take aim at different network layers, so it's important to protect your network in a holistic way.

There are three main types of DDoS attacks that cybercriminals use on their targets:



1. Volumetric attacks

The goal of this style of attack is to overwhelm the target's bandwidth with a high volume of botnet traffic, keeping legitimate traffic from accessing the network. These kinds of attacks are immediately obvious to the victim and other upstream providers and are sometimes a cover-up for a larger cybercrime.



2. Protocol attacks


These attacks target vulnerabilities in layer 3 and 4 protocol communications infrastructure like firewalls and web servers by exhausting them with malicious connection requests. These attacks are often overlooked as they're less obvious.



3. Application-layer attacks

This style of attack aims to consume server and network resources by capitalizing on weaknesses at the application layer (layer 7). The targets here are software or cloud-based web applications. These kinds of attacks are among the most highly publicized and common and are difficult to prevent.

Because these three types of attacks target different components of the network, it's critical to protect your website presence plus your network and applications.



DDoS attack activity has grown to the point where a specialized solution is needed to combat it.

4. What type of DDoS protection is right for my business?

So now you know what attackers can target, how do you protect your business from DDoS attacks?

At a basic level, you'll want to have excess bandwidth available to you in case attackers try to overwhelm your existing web resources with illegitimate traffic. That way, you can keep the lights on even in the face of an attack.

There are two ways you can protect against these kinds of attacks:



1. Purchase extra bandwidth

The first option would be to have extra bandwidth on deck in case of traffic surges to help outscale attackers. This won't prevent a DDoS attack from happening, but it could buy you some time to strategize in the face of an attack.



2. Use a CDN

A Content Delivery Network, or CDN, will also allow you to outscale the bad guys by redirecting traffic to global servers to offload some of the traffic and make surges more manageable.

These options will help create a cushion around your existing capacity and offer some protection against volumetric attacks, but won't protect you against DDoS attacks on network or application-layer technologies.

In addition, firewalls are sometimes cited as a way to add protection. However, firewalls are not sufficient to combat DDoS attacks, but they do protect against some cyber attack activity. DDoS attack activity has grown to the point where a specialized solution is needed to combat it.



On-premises DDoS protection solutions are best for large organizations operating on-site.

There are two types of solutions that can help guard against more sophisticated attacks: on-premises and off-premises.

On-premises DDoS protection solutions

This kind of solution refers to hardware that's positioned inside the network and is a powerful opponent to attacks on the premises of the organization. These are best used by large organizations with a majority of their workers working and operating company equipment on-site. They're also best suited for regulated industries like healthcare and finance that face restrictions against moving IT workloads to the cloud and organizations that own and operate their own existing data centers.



Pros:

- Great protection on-premises
- More operational control
- Low latency
- Meets regulatory requirements



Cons:

- Size and bandwidth constraints
- Require manual deployment
- High ownership costs
- Labor and maintenance costs
- Poor protection against network-layer attacks

**Off-premises
DDoS
protection
solutions
provide low
cost, scalable,
fully managed
protection for
any kind of
business.**

Off-premises DDoS protection solutions

There are two main types of off-premises DDoS solutions: network-based and cloud-based.



Network-based

These solutions provide ISP-based off-premises protection against network-layer attacks. They provide a good supplement to on-premises protection or additional capacity, depending on the organization's needs.



Cloud-based

These solutions do not require any hardware and offer great application-layer protection off-premises. This kind of solution is preferable for organizations with a dispersed workforce that typically works off-premises and those who are moving to the cloud or operate mainly from the cloud.



Pros:

- Little to no hardware is required.
- Managed and maintained by DDoS protection professionals.
- Lower cost compared to on-premises solutions with flexible subscription packages.
- Scalable bandwidth.
- Great application-level filtering.



Cons:

- Latency can be a drawback since all traffic is routed through the provider.

Most organizations will find an off-premises solution to be the better option. However, if your organization requires a combination of both, it's possible to deploy a hybrid solution to provide both the scale of off-premises solutions and the latency of on-premises ones.

Budget is a top consideration for every organization.

5. How much will DDoS protection cost?

Different types of solutions are associated with different costs and cost structures.



1. Content Delivery Network

Using a CDN can cost anywhere from a few hundred to a few thousand dollars depending on how many terabytes of additional capacity you need. This should be included in your budget if you have a website presence for baseline protection.



2. Off-premises

Cloud and network-based solutions often involve monthly subscriptions tiered based on traffic and usage. In general, you can expect to pay a couple thousand dollars a month on this kind of service, depending on the vendor and the level of coverage you need.



3. On-premises

As previously mentioned, on-premises solutions are much more expensive to set up and maintain. On-premises solutions typically involve expensive hardware that costs well over \$100,000, lending to high start-up costs. In addition, teams that install on-premises solutions require on-site support and maintenance and dedicated staff to manage devices and equipment, adding to the cost of management. This is all not to mention the cost of utilities like power, networking, and cooling needed to keep on-premises solutions running.

It's tough to say with confidence what exactly you will end up paying for, but if you do fall victim to a DDoS attack, it will undoubtedly cost you.



**The time to
protect your
business
against the
growing DDoS
threat is now.**

Dependable network-based DDoS Protection from Zayo

Zayo's network-based DDoS Protection service is available to any customer with Zayo Internet service. Activating Zayo DDoS Protection is fast and seamless – all you need to do is send a list of protected IP addresses to get started.

Once you begin your service with us, you'll be able to enjoy all of the benefits of Zayo DDoS Protection including:



Mitigation at the core of our network and the peering edge.

Our solution leverages our Tier-1 network and 30Tb+ of peering capacity.



Latency-free protection for normal traffic.

Since our solution sits inline with our network and traffic is monitored as it enters the network in its peering edge routers, there is no redirection of traffic through a monitoring device not in the direct traffic flow.



Filtering through global scrubbing centers.

Illegitimate traffic is removed at our scrubbing centers allowing only clean traffic to filter through to you.



Insights from our customer portal.

This includes real-time traffic analysis, enhanced reporting, and solution management.



24/7/365 support from our knowledgeable experts.

Our cybersecurity experts are available to answer any questions you have and can help optimize your security solution to your business's unique needs.

**You can learn more about our DDoS
Protection solution at**

zayo.com/solutions/ddos-protection

Citations

1. "Annual Threat Report 2020." Nexusguard Blog,
<https://blog.nexusguard.com/threat-report/annual-threat-report-2020>. Accessed 2 March 2022.
2. Lowry, LeeAnne. "U.N. Official Warns Cybercrime Up 600% During COVID-19 Pandemic."
Newsy, 23 May 2020,
<https://www.newsy.com/stories/u-n-warns-cybercrime-up-600-during-covid-19-pandemic/>.
Accessed 9 March 2022.
3. Moskovska, Andriana. "DDoS Statistics 2021: Dynamics of DDoS Attacks In Australia."
TakeATumble, 29 December 2021,
<https://takeatumble.com.au/insights/security/ddos-statistics/>. Accessed 2 March 2022.
4. Toth, Jozef. "13 impressive statistics on user experience | Inside Design Blog." InVision, 24
November 2015, <https://www.invisionapp.com/inside-design/statistics-on-user-experience/>.
Accessed 2 March 2022.