White Paper

Protecting against DDoS attacks with Citrix

In this white paper, we will explore the growth and trends of DDoS attacks as well as how they impact businesses. A DDoS, or denial-of-service, attack is a cyberattack in which the perpetrator seeks to make a resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet. DDoS attacks aim to overload (or exhaust) a business's digital resources and prevent them from performing normally.

Even after 25 years, DDoS attacks still pose a huge security risk for every business. This is in large part because they are relatively easy and cheap to launch. We'll discuss the main factors of a DDoS attack and how the Citrix Web App and API Protection service can keep your company protected— ensuring data integrity, avoiding business disruption, and meeting legal compliance standards.

DDoS Trends and Evolution

The pandemic has dramatically increased online e-commerce, internet traffic, and a growth in data traffic in general. Forbes details an Adobe report estimating that COVID-19 accelerated e-commerce growth by four to six years. This huge rush to get online has also expanded the opportunity for cyberattacks, as attackers target the unprepared. DDoS attacks increased in size by 30 percent in 2020 and more than 70 percent of enterprises report being victims of DDoS attacks. Therefore, it's not surprising that a DDoS attack is the number one reason why a business goes offline and one of the greatest concerns of security executives.

There are the three main categories of DDoS attacks:

- **Volumetric attacks** attempt to flood the network with traffic and fill the pipes to prevent legitimate connections from getting through. An effective service mitigates these types of attacks, which include Ping of Death attack, ICMP Flood, IP/ICMP Fragmentation, IPSec Flood, and others.
- **Connection protocol attacks** target network devices like routers, firewalls, and load balancers and attempt to fill their connection tables. A successful mitigation service blocks spurious traffic and ensures availability for legitimate connections. Common attacks that Citrix can mitigate include SYN floods and UDP floods.
- **Application-layer attacks** target applications or services at L7. These attacks can easily bring down an app with a low rate of seemingly legitimate requests. This makes them difficult to detect. An intelligent defense safeguards against application-layer attacks including the popular HTTP GET Flood and DNS amplification attacks.

There is no doubt that DDoS attacks are on the rise, Cambridge University's Cybercrime Centre reports there were 30,000 attacks per day in 2020. That's nearly 11M over the course of the year, which is up 20% from the year before.

A big driver for this growth is because it is simple to launch DDoS attacks. It is astonishingly cheap and easy to orchestrate a DDoS attack. A quick search on the dark web for DDoS services and a few clicks is all it takes. According to anti-virus software vendor Kaspersky, it can cost as little $20 per hour to attack a subject with a basic attack. Of course, more sophisticated attacks that use a mixture of techniques will cost more, but it is still very cheap when compared with the damage that can be done.

A key reason for the decline in the cost of launching DDoS attacks is the proliferation of IoT devices for bot networks. In the hands of the general public, the lack of security experience means that device owners often don't change the default credentials, which leaves them open to compromise. Compromised devices can be recruited into large botnets controlled by cyber criminals, who farm out services to the highest bidder. Those using the services can carry out DDoS attacks and retain anonymity, which make it difficult to track them down.

In February 2020 AWS mitigated a massive DDoS attack of 2.3 Tbps. Google has also recently revealed that it faced a long-term attack in 2017 that peaked at 2.5 Tbps. Moreover, Yandex, the Russian tech giant, reported an attack of

22 million requests per second in August 2021.

Attacks are increasing in size, and it seems inevitable that we will witness the world's first attack in excess of 3 Tbps soon. DDoS attacks are getting more problematic not only size, but in sophistication as well. This is a key reason why more businesses are focusing on DDoS defenses.

In addition to the actual mechanics of the DDoS attack itself, the strategy of the attacker needs to be considered. DDoS attacks have also been used as a diversion to attract the attention of the security team so that it is easier to attempt a data breach using ransomware or another attack vector.

Ransom DDoS Attacks Are On the Rise

Although they are not new, ransom DDoS attacks have surged in popularity. Ransom notes often accompany, or precede, a DDoS attack to demand payment to either stop an ongoing attack or to avoid the launch of an attack. In the latter case, it is possible that the capability to launch a full-scale attack does not exist, but it is unwise for a business to make this presumption. Ransom DDoS seems especially prevalent in the healthcare and finance industries as you'd expect.

In many cases ransom notes may lay claim to an affiliation with famous hacker groups like Fancy Bear, Lazarus, or others to lend credibility. The attackers may also take credit for a previously known attack, or one that is currently ongoing – again to build credibility. Sometimes the extortion note is accompanied by a small DDoS attack to prove that the group is serious and capable. However, in many cases it begins with a real attack.

Ransom DDoS makes it difficult for a company to assess what to do next. They wrestle with questions such as: What is the ransom size? Can we afford to pay it - can we afford not to? If we pay it, will we be viewed as an easy target in the future? Should we inform the authorities? Can we withstand a DDoS attack?

As mentioned, healthcare and finance companies have become focused targets for DDoS attacks and ransom attacks. This stems from the fact that they have a higher regulatory obligation to maintain security and, subsequently, they face stiffer penalties for failing to keep systems active or – even worse – allowing a data breach. For attackers, this increases their confidence that a ransom will be paid.

Ransom DDoS attacks have seen major growth since their early days. Back when ransom DDoS was first used, it was often to gain clout or used as an act of "hacktivism" against a company that upset people with their business practices. The overwhelming trend of DDoS ransom attacks for monetary gain should be a concerning development for all IT executives. With the birth of cryptocurrency, this movement has only been amplified. Not only can hackers act more freely with an untraceable and legitimate form of payment, but now anyone with access to the dark web can anonymously hire DDoS attacks with ease.

DDoS Attacks Hurt Your Business in Many Ways

How do DDoS attacks impact business? Because businesses rely on applications and digital services, any disruption by a large-scale DDoS attack can be potentially disastrous for any company. The potential for revenue loss caused by lack of functionality of IT systems such as ecommerce engines, web applications, and online portals can quite literally be an existential threat.

The impact to business usually falls into four categories: business disruption, financial cost, reputation damage, and legal exposure.

- Business disruption impact is the loss through the inability to do business and includes lost revenue and reduced

productivity. While it is difficult to put a definitive monetary value on lost business or lost productivity because of downtime, Tech Insurance, a liability insurance company popular in the tech industry, reported enterprises can reach the hundreds of thousands of dollars per hour and that SMBs range between $8,000 and $74,000 per hour. Of course, the actual amount will vary by industry and by the volume of online transactions a business carries out. And as DDoS attacks become more prevalent, the risk associated with lost business grows accordingly.

- Financial costs are expenditures associated with having to restore services and manage operations to keep a business active during a DDoS attack. These costs can be much higher than the direct loss related to the inability to trade. A survey by Kaspersky labs found that on average the total cost of a DDoS attack is $2M for an enterprise and $120,000 for an SMB.
- Reputation damage, although intangible, is one of the biggest risks businesses face due to a DDoS attack. Businesses tend to suffer the most reputation damage when intellectual property or customer data is lost. Sure, customers get dissatisfied when they are not able to access a site, or when a DDoS attack causes performance to degrade, but they get very angry when their personal data is stolen. Customers will likely perceive compromised businesses as incapable of protecting their data and sensitive information. While a business may be able to restore that trust, it may require a big investment in marketing and media relations.
- Legal costs arise when the attack causes violations of law or when it impacts another business, which can increase liability. When an SLA has been breached because of an attack, a third-party might sue for damages. And there is a chance that customers may sue if they have lost money or if the attack facilitated a data breach. Additionally, as we mentioned with healthcare and finance, certain industries may face additional penalties imposed by government agencies.

Recent Key DDoS Attacks

As previously discussed, one of the largest known attacks occurred in Feb 2020 against an AWS customers. The UDP/CLDAP reflection attack was staggering to say the least, being a massive 44% increase from the previous reported largest attack. The Yandex attack extended this in terms of requests per second. It's clear that with the ease of launching a DDoS attack, no business is safe.

A great example of industry targeting is the 2020 attack against the New Zealand stock exchange (NZSE). The attack took place over the course of a few days, with the NZSE services being intermittently taken down. While NZSE was occupied dealing with the DDoS caused outages, the attacker also attempted to breach the New Zealand Stock Exchange's data. Stories like these make it abundantly clear that industries with much to lose must take extra care with their security requirements.

In 2021 an attack was launched against the Belgium Government, which is host of the European Union Headquarters. A well-targeted attack such as this one is effective in being able to cripple an entire government, even if only temporarily. EU Parliament meetings were disrupted and 200+ Belgian government institutions affected, including law enforcement and other key government functions.

The Considerations of an Effective DDoS Defense

The foundation of a successful DDoS mitigation service must be built upon a powerful and sophisticated network. A poor network would result in high latency for customers, or potentially even lack the most important principle of DDoS mitigation; the ability to scrub massive amounts of bad traffic. There are 6 considerations to an effective DDoS Defense.

1. Block Bad Traffic: The first and foremost goal of DDoS defense is to identify and block spurious traffic.
2. Allow Legitimate Traffic: Defenses must be intelligent to identify and allow legitimate traffic. By only blocking

bad traffic, it can get tricky knowing which traffic is bad and which is good.

3. Choice of Protection Models – Cloud Delivered vs. On-Prem: An on-premises DDoS defense system can be useful, but it is unlikely to cope with modern DDoS attacks. A cloud protection model is much more scalable, as well as simplifying deployment and management.
4. Highly Scalable: An effective DDoS defense must scale to scrub data for any size attack. A cloud-delivered DDoS mitigation service provides scalable protection for those scenarios where the influx of traffic would have surpassed on-prem capabilities.
5. Global Coverage: Global presence is important for a successful DDoS mitigation service. Globally distributed points of presence (PoPs) help minimize the inevitable added latency that scrubbing introduces.
6. On-Demand vs. Always-On: An effective DDoS mitigation service should offer the choice of always-on scrubbing as well as on-demand scrubbing. Different businesses have different requirements and need to ensure that they have a solution to fit their needs. An effective solution must provide choice.

Citrix Solution for DDoS Protection - A SaaS Solution

This service offering is customizable, offering choice such as on-demand and always-on so customers can meet their specific security needs, all while providing the ease of use of a cloud delivered service model. The key benefits of the Citrix DDoS Protection Service are its ability to protect against many different attack vectors, its ease of use and scalability, its truly outstanding network coverage, and all delivered as a service without capital expense outlay.

Comprehensive Protection against DDoS Attack Vectors

Citrix protects against the three main categories of DDoS attack: volumetric, connection protocol, and application layer. The solution can prevent the filling of pipes that happens in volumetric attacks, it will protect networking equipment and connection tables from overfilling as seen in connection protocol attacks, and safeguards applications from sophisticated application layer attacks.

Further, a growing trend in DDoS attacks and perhaps the most dangerous of all, is to combine elements of all three of the attack categories. These multi-vector attacks can be difficult to deal with, for example, you may be scrubbing large amounts of traffic filling the pipe and think that you're winning, only for the firewalls to succumb to connection exhaustion or the application to be hit by a more subtle attack. Because of its intelligent approach to DDoS protection, Citrix is fully capable of mitigating multi-vector attacks.

Citrix defends against all these attacks and protects applications whether they are deployed in the cloud, on-prem, or both. In nearly all of these attacks the application, server or network may receive hundreds or thousands of requests per second and become so busy processing them that it cannot respond to legitimate requests. Or, the service may respond so slowly that it is effectively unusable.

DDoS Protection as a Cloud-Delivered Service

A huge benefit to users of the Citrix Web Application and API Protection service is the ease of deployment, management, and scalability. Onboarding is simple and requires minimal setup. We've simplified processes for you, so configuring rules and policies is intuitive. Moreover, there is none of the operational overhead associated with appliance installation or maintenance. As a service, the latest protections are automatically available without manual upgrades. Additionally, it takes only 30 minutes or less to get started, helping to protect you right away. Also, as you grow, the service grows with you. Scalability is as simple as a license upgrade; the process of increasing capacity takes only minutes. The Citrix DDoS solution dramatically reduces the operational complexity of mitigating DDoS attacks.

Global Coverage and Scale

With 14 global points of presence (PoPs) providing more than 12 Terabits per second of scrubbing capacity, the infrastructure is designed to handle even the largest DDoS attacks. In addition to this, every global PoP location features multiple connections to the largest Tier 1 and Tier 2 service providers to ensure that your applications continue to perform as they should. If you have questions or problems, Citrix SOC experts are available to help you, 24/7/365.

14 PoPs across the globe minimize latency between your users and your applications

Always-On and On-Demand Options to Suit Your Budget, Security Strategy, and Needs

When you make a DDoS defense selection, they must decide whether to have always-on vs. on-demand protection. With Citrix always-on mitigation, traffic is continuously routed to our scrubbing centers. The downside of always-on is that it does add latency to every request. However Citrix's global coverage, minimizes this added latency. The downside of on-demand protection is the fact that traffic must be redirected to the scrubbing centers when an attack occurs. This leaves a small amount of exposure and the chance of an outage at the start of an attack. That said, the exposure is minimal, as Citrix can detect the attack and divert traffic in only a few minutes.

Integrated Solutions to Fully Secure Your Business

A stand-alone DDoS protection service is great at protecting against DDoS-specific attacks. However, businesses require more comprehensive protection for their applications and APIs. Some businesses prefer to have their WAF, bot management, and API protection on-premises. An integrated solution with DDoS mitigation can provide complete protection at a single point and should be a consideration. The integrated solution can safeguard valuable business

data assets against multi-vector attacks, minimize complexity, and reduce TCO.

Citrix is focused on meeting business needs and has built the above choices into their offering. Regardless of your requirements, Citrix can offer the right solution suited to their security requirements. With the choice of always-on and on-demand, as well as integrated and standalone DDoS protection, Citrix offers a great range of choice to help you get the protection that's right for you.

Why Citrix?

The Citrix DDoS Protection Service offers top-tier protection against DDoS attacks. The key benefits Citrix provides are:

- Comprehensive Protection against DDoS Attack Vectors: Protects against all forms of DDoS attacks, even multi-vector.
- DDoS as a Cloud-Delivered Service: Protects applications deployed in cloud, multi-cloud, datacenter, or hybrid.
- Global Coverage and Scale: 12 Tbps actual scrubbing capability is one of the best and offers a true worldwide presence to deliver clean traffic globally with minimal added latency. Ability to quickly and easily add on more Application and API security with simple license upgrade
- Always-on and On-demand Options to Suit Your Budget, Security Strategy, and Needs: Allow the business to choose whether data will be scrubbed at all times or only once an attack is launched.
- Integrated Solutions to Fully Secure Your Business: Ability to quickly protect against just DDoS or protect all application attack vectors.

Citrix DDoS protection offers 24x7x365 SOC Support backed by SLAs, and its strong network and advanced packet filtering can protect you from both massive and multi-vector attacks. It is built to be easy to use and delivered to wherever your data is. Finally, the way in which it is delivered and sold is beneficial to you, allowing you to customize the solution to fit your budgets without compromising your security needs.

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States