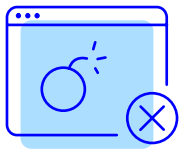
Three ways to prepare for and beat DDoS attacks

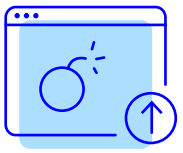
INSTART

The World Economic Forum[1] recently ranked cyber attacks alongside the climate crisis and weapons of mass destruction as one of the greatest threats of 2019. One of the most common cyber attacks[2] is a distributed denial of service, also known as DDoS.

DDoS attacks prevent access to a website, web app, or other online resource by overwhelming the application server with requests. Every business is susceptible. A competitor, cybercriminal, or even a disgruntled employee can hire a hacker to unleash a DDoS attack for as little as $5 an hour.[3]



Cox recently warned business owners that an average DDoS attack is enough to take most websites completely offline.[3]

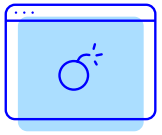


Kaspersky, a multinational cybersecurity and anti-virus provider recently reported an 84 percent increase in the total number of DDoS attacks.[4]

Some DDoS attacks are simply meant to be a nuisance, but others are more sinister. Approximately one-third[5] of DDoS attacks include a network intrusion, such as installing malware or stealing data. Even if the attack doesn't include a data breach, losing control of your web presence can erode consumer trust.

DDoS attacks can last a **few hours** or even **several days**.[6]

The cost of a DDoS attack averages **$20,000 to $40,000** per hour in mitigation and lost revenue.[3]



After a DDoS attack, **47 percent** of cases led to virus injection, **43 percent** led to malware activation, and **32 percent** resulted in data theft.[7]

Three ways to prevent and defend against DDoS attacks

The ease and low cost of initiating a DDoS assault means every business needs to establish a secure perimeter, regardless of industry or business size. For cybercriminals, there is no such thing as a "too small" or "off the radar" website.

The Honeynet Project, a non-profit security research group, created a nearly-invisible web server (it wasn't even connected to a domain) to measure the prevalence of bad actors on the internet. The server was attacked more than 250,000 times[8] in 24 hours.

Don't get caught off guard. The easiest, most cost-effective way to beat a DDoS attack is by being prepared. Here are the three things you need to know about DDoS mitigation to protect your organization.

1. Detect: Accuracy prevents downtime

Early detection is one of the best ways to defend against DDoS attacks. When an attack is quickly and accurately identified, downtime can be avoided completely.

Effective monitoring is key. A detection system must be able to differentiate between a spike in consumer demand and an attack from a botnet. The best DDoS detection systems incorporate continuous monitoring and intelligent technology that identify attack vectors and surface actionable data for attack prevention and deflection.

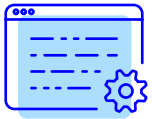
Instart Web Security compiles results from multiple rules to reduce false positives and improve threat detection accuracy. In addition, Instart is also able to block or rate-limit all HTTP and HTTPS traffic connecting to your origin with simple conditional rules, enabling layer 3 and 4 protection and layer 7 protection. Our technology combines an intelligent edge with powerful insights from the browser to detect and stop even the most sophisticated attacks.

2. Protect: Protection from application to the browser is the only way

A web application firewall (WAF) can defend against some DDoS attacks, but is not a complete solution. To fully protect your business, you need a WAF plus deep client-side capabilities that extend into the browser to control third-party and cloud-based content.

86 percent of DDoS attacks use multiple attack types (UDP floods, HTTP flood, application layer/ layer 7, advanced persistent DoS, etc.)[3]

DDoS attacks were ranked as the **number one** threat in a recent survey of security professionals, and **52 percent** had already experienced an attack[9]



An Amazon Web Services server instance running on a CMS such as WordPress can be brought down by as few as **500 HTTP requests** per second[10]

Instart offers industry-leading DDoS protection that pairs innovative technology with a scalable, cloud-based proxy. Defend against even the largest DDoS attacks with always on DDoS protection across layers 3 and 4, layer 7, network-wide HTTP and HTTPS traffic absorption, advanced caching, and custom security rules.

3. Eradicate: Effective security is essential

Once compromised, mitigating the impact of a DDoS attack is the only way to get your web applications back online. When an attack is underway, effective security can be the difference between a hectic day for IT versus explaining to customers why your website was offline for hours — and losing hundreds of thousands in revenue.

WAFs alone cannot protect against or defuse a DDoS attack. Play offense instead of defense with a modern security solution from Instart that includes:

- ✓ Rate-limiting capabilities to block traffic by IP, geographic location, or user agent
- ✓ Detailed, real-time security analytics
- ✓ Bot detection and mitigation
- ✓ Independent, overlapping layers of security
- ✓ An intelligent CDN that can throttle attack traffic, monitor, and deliver “clean” traffic

DDoS protection from Instart

Instart creates a proxy between your application's incoming traffic, shielding your origin servers from the wilds of the web and reducing the security burden for your organization. With Instart security services, you can secure all the entry points into your web application servers, offering end-to-end protection from the browser where your customers and attackers interact with your site, to the edge, all the way to your application infrastructure. Defend against the most common and most sophisticated cyber attacks including DDoS, Cross-Site Scripting (XSS), SQL Injection (SQLi), and others.

Learn more about how Instart's cloud-based security services provide the protection you need without sacrificing performance.

Request a demo

INSTART

www.instart.com

Sources:

1 www.weforum.org
2 www.cisco.com
3 www.coxblue.com
4 securelist.com
5 www.infosecurity-magazine.com
6 usa.kaspersky.com
7 ns-cdn.neustar.biz
8 www.honeynet.org
9 www.information-age.com
10 www.indusface.com