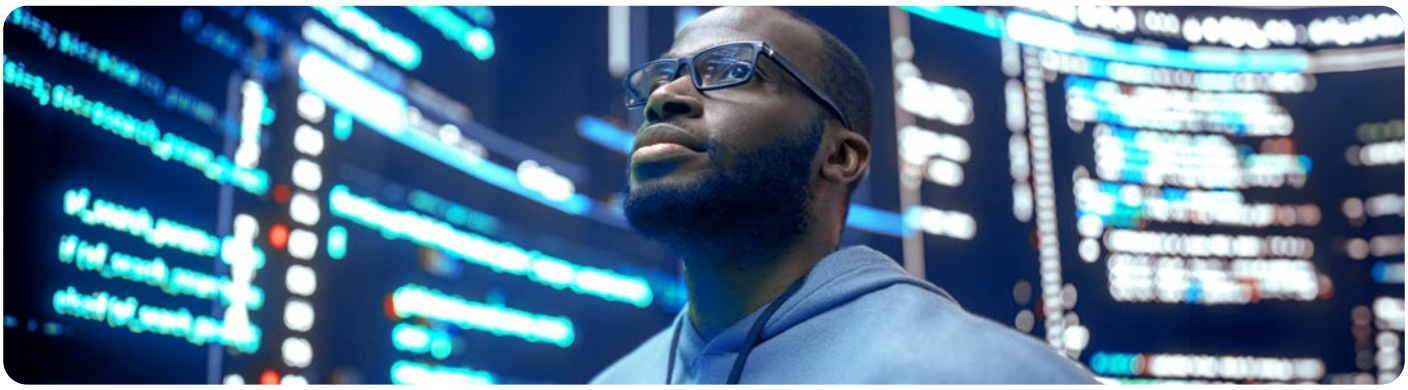
A reality check on DDoS attacks

Seven assumptions that expose your business to risk



The cyber threat landscape is changing rapidly, with organizations experiencing more complex attacks than ever before. DDoS attacks are among the most aggressive in nature and volume, with the number of attacks growing by more than 150% in 2022[1]. Despite this reality, many organizations believe that DDoS attacks are an easy problem to solve. Below are seven realities that show this is not the case.

Reality 1: All industries are subject to an attack; no one is immune

While some industries are more prone to attacks, any industry can be a target. The ease of access and low cost of initiating attacks make it easy for hackers to launch an attack against any business or individual, in any industry. Web application and API attacks grew exponentially throughout 2022. This widened the threat landscape and made it easier to access any industry.

Reality 2: DDoS attacks result in more than just website graffiti

DDoS attacks are often a diversion for more lethal attacks. While the SOC is busy responding to the DDoS, attackers may be running other tactics to capture data or navigating (lateralization) within the client system. Hence, it is critical to reduce what is often perceived as noise in order to enable your SOC to do their actual job, i.e., detecting meaningful threats.

Reality 3: Firewalls alone do not provide enough protection

Firewalls and IPS sometimes have DDoS features, which are useful to detect some malicious IPs, but they will be useless against volumetric attacks or Layer 7 attacks. It is advisable to have a web application firewall to detect OWASP 10 attacks, Layer 7 exploitations, in conjunction with a DDoS protection.

Reality 4: DDoS attacks are not only volumetric

While the number of volumetric network layer attacks are higher, the number of slow-paced application layer attacks are also on the rise. Multi-vector attacks are becoming more common; these combine high-volume, network-layer attacks with sophisticated application-layer attacks. Web application and API attacks increased by 128% from 2021 to 2022.[1]

Reality 5: A DDoS attack will impact much more than your website

Any asset connected to the Internet can be impacted: supply chain, point of sale, transaction processing, patient records and customer service, to name a few. All external-facing systems need protection no matter where they are managed. Access to your online systems can even be blocked if your domain name servers (DNS) are attacked.

Reality 6: Organizations of all sizes are targets for an attack

DDoS attacks can hit any business regardless of its size. With the emergence of DDoS for ransom (RDDoS), smaller companies become easier targets because they have limited IT resources to deal with these attacks.

Reality 7: DDoS solutions must be at the core of your cybersecurity budget planning

With the growing number of attacks and level of sophistication, the impact on businesses is much more than lost revenue; reputation damage, customer churn, and legal implications are all considerable risks. No matter the attack frequency, duration or size, unprotected organizations experienced an average cost of $200,000 per DDoS attack[2] —and that is before considering attacks associated with ransomware. In 2020, the average cost of ransomware attacks in Canada was almost $2 million.[3]

Protect your network and your business with Bell

As Canada's largest network operator, Bell has a unique vantage point over the DDoS threat landscape – and can provide protection to detect, mitigate, and filter DDoS attacks.

For an evaluation to see if your business is at risk, request a call from a Bell cybersecurity expert.

For more information about DDoS and network security, visit bell.ca/DDoS

[1] 2022 Global Threat Analysis Report – Radware
[2] Financial Post: DDoS Attacks in H1 2023 Up 200% from 2022 According to New Zayo Data
[3] 2020 Cyberthreat Defense Report (CDR)