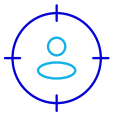
SEGRA

DDoS Edge Protect: **Myth vs Fact**

1 WE WILL NOT BECOME A TARGET. OUR BUSINESS IS TOO SMALL.

DDoS attacks do not discriminate. Any organization, big or small, is in danger of experiencing the risks associated with a DDoS attack. Any organization that hasn't taken the necessary steps to protect against these types of attacks could be at serious risk.

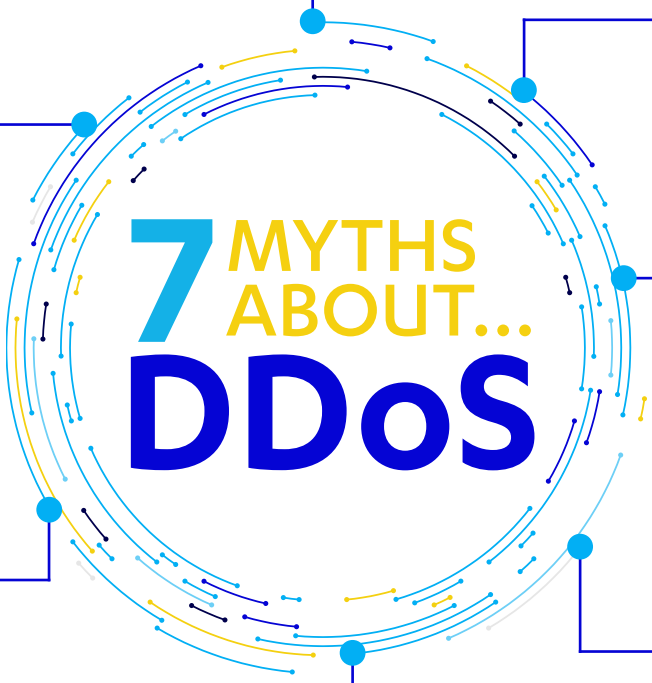


2 OUR FIREWALL CAN PROTECT AGAINST DDoS ATTACKS.

Firewalls cannot protect against complex DDoS attacks, and instead act as DDoS entry points. Attacks pass right through open firewall ports which are intended to allow access to legitimate users.

3 MY WEB PROPERTIES ARE MANAGED BY A HOSTING PROVIDER. I DO NOT HAVE TO WORRY ABOUT DDoS.

The sheer volume of customers within a hosting environment increases attack surface, and innocent bystanders can become collateral damage when an attack occurs.



4 DDoS SOLUTIONS ARE NOT WORTH THE INVESTMENT.

A DDoS attack can cost millions of dollars in lost business, brand damage, threat exposure and customer attrition, and even can lead to a business shutting down for good. According to a study from the Ponemon Institute, the average downtime due to a DDoS attack is 54 minutes with an average cost of $22,000 per minute. On average DDoS attacks are costing companies close to 1.2 million dollars per attack.

5 MY INDUSTRY IS NOT A TARGET FOR A DDoS ATTACK.

Industry does not matter. Whether you are n the financial, retail, manufacturing or services industry, you are a target for DDoS attacks. The drivers for launching attacks are far-ranging and difficult to pinpoint in many cases - anyone can become a victim at any time.

6 ONCE I HAVE DDOS PROTECTION IN PLACE, I DON'T NEED TO WORRY ABOUT IT ANYMORE.

DDoS Protection requires ongoing management and updates. Attackers constantly evolve their methods, so defenses must be regularly reviewed and updated.

7 WORK FROM HOME FLEXIBILITY, ADDS DDOS COMPLEXITY.

The rise of remote work has increased the attack surface, leading to more frequent and sophisticated cyber threats. Inadequate security for remote employees can make Business WANs more vulnerable, risking losses in time, finances, clientele, and reputation due to successful DDoS attacks.