

TOP DDoS ATTACK MYTHBUSTERS



MYTH

My on-premises DDoS solution has my company protected against all DDoS attacks

My company isn't a target for DDoS attacks

My firewall has my company protected against DDoS attacks

DDoS attacks are simple and use only a single vector

Our business is too small and will not come under DDoS attacks

DDoS attacks are only volumetric in nature

DDoS solutions aren't worth the investment

There is no financial goal around DDoS attacks

TRUTH

One of the largest DDoS attacks recorded by F5 approached 450+ Gbps, which would easily overwhelm any on-premises DDoS deployment. F5 recommends a hybrid approach of both on-premises and cloud scrubbing.



The fastest growing DDoS attack type is volumetric.¹

All industries come under DDoS attacks with education and professional services, emerging as new attack sectors. Attack motivation varies from hacktivism to financially motivated cybercriminals.

90%

90% of reported DDoS incidents are in the professional sector, followed by 81% in education.²

Unfortunately, firewalls and IPSs can't distinguish between malicious and legitimate users, allowing DDoS attacks to pass right through open firewall ports. In addition, most firewalls aren't able to handle volumetric DDoS attacks.



F5's surveys found that more than 40% of DDoS attacks pass through current on-premises firewalls.¹

76% of DDoS attacks are multi-vector and take sophisticated tools and knowledge to mitigate.



DDoS attacks are more likely to be multi-vector attacks than single-vector attacks.¹

DDoS attacks don't discriminate. Any organization, big or small, is in danger of experiencing the risks associated with a DDoS attack.



On average, an organization has experienced at least one DDoS attack in the last year.³

The most damaging DDoS attacks mix brute force (volumetric) attacks with targeted, application-specific attacks.



Application-layer attacks comprise about 19% of all reported DDoS attacks.¹

DDoS solutions are worth the investment, especially when you need mitigation. Be prepared to keep your business online and shine for execs.

\$\$\$

45% of organizations were DDoS-attacked at least once in the past year, at an average cost of \$200K–\$500K per hour.³

DDoS attacks are sometimes used as a mode of distraction to veil some other attack taking place in the background (such as account takeover).

90%

90% of all multi-vector cyberattacks involve a DDoS smokescreen.¹

¹F5 SILVERLINE, ²2016 DATA BREACH INVESTIGATIONS REPORT, VERIZON, ³FORRESTER, UNDERSTAND THE BUSINESS IMPACT AND COST OF A BREACH, 2015