DON'T LET DDOS PREVENTION & MITIGATION SCARE YOU

What you should be able to answer with confidence.

It's no secret that DDoS attacks are on the rise again. Countless articles detail the recent misfortunes of organizations suffering downtime due to a DDoS attack. Falling victim to an attack could be catastrophic, causing organizations to lose revenue or paralyze an organization's network.

By the numbers...

ATTACK FREQUENCY
25% increase in DDoS Attacks[1]

ATTACK SIZE
Grew by 275% in first half of 2020[2]

COST OF DDoS ATTACK
$20,000-$40,000 US per hour[3]

While the numbers above might seem scary, organizations can prepare now to protect themselves from a future DDoS attack.

Here are 5 areas organizations should have control over and be able to address confidently, to reduce the time to remediation for a DDoS attack.

What type of visibility do you have when you're under a DDoS attack?
Being able to see what is happening at all times across your network is key to any security strategy. According to a 2020 survey[4], 59% of cybersecurity professionals believe that lack of network visibility poses a high or very high risk to their operations. Network visibility ensures that network and security teams can see what is happening and respond appropriately. Having 100% visibility also ensures you can see your entire environment(s) in a single-pane-of-glass.

Do you know what type of attack it is? Do you know the size?
Knowing what type of attack it is and the size could help your organization save a lot of money and hassle. Not all attacks are the same, and you may be able to handle some attacks in house with your own equipment. Knowledge is power and can help keep costs down and avoid unnecessary steps if you're able to handle it in house.

What means do you have of taking control and re-routing traffic to your DDoS provider(s)? Ideally, organizations should choose when to route on to the provider if an attack reaches a specific threshold. How fast are you able to re-route your traffic? Can you do this with a rule-based threshold or a DNS redirect?

Where is the attack coming from? Is it coming from inside the network?
This seems like a simple enough question to answer. Understanding where the attack originates from helps understand what security practices need to be shored up so that it doesn't leave the organization vulnerable to future attacks.

Are you actually under attack?
Not all attacks behave the same way, and it can be difficult to tell if it is a DDoS attack. Some attacks are too small to detect. But what if you are not sure? Having a definitive confirmation from your security tools is another way and should be the first to tell you that you are under attack - not your customer or your employees.

Take Back Control Of Your DDoS Mitigation Strategy

The Netography Security Platform can provide you with better visibility and put you back in control of the situation to detect and remediate cyber threats. To learn more about how Netography can help streamline your DDoS mitigation strategy, visit www.netography.com/ddos

NETOGRAPHY

[1] Netscout , Threat Intelligence Report: Cybercrime exploiting a Pandemic - https://www.netscout.com/threatreport
[2] Neutstar, CyberThreats & Trends Reports - https://www.home.neustar/resources/whitepapers/cyber-threats-and-trends-report-2020-first-half
[3] Cox Blue, 12 DDoS Statistics that should concern business leaders - https://www.coxblue.com/12-ddos-statistics-that-should-concern-business-leaders/
[4] Sans, 2020 Sans Network Visibility & Detection Survey - https://www.sans.org/reading-room/whitepapers/detection/paper/39490