EXECUTIVE BRIEF

# DDoS mitigation:

The frequency and duration of volumetric attacks require a greater focus on network security

## The current DDoS threat has:

**Greater incidence:** The number of DDoS incidents reached 7.9 million attacks in the first half of 2023 alone, representing a 31% year-over-year increase.[2]

**Longer duration:** In 2023, most attacks lasted 5 to 10 minutes, and the longest attack was 7 days.[3]

**More points of origin:** The number of Internet of Things (IoT) connected devices worldwide is expected to reach almost 30 billion by 2030.[4]

Distributed denial of service (DDoS) attacks are designed to flood connectivity to a network, application or service so that the intended users cannot access their resources. These attacks are initiated with the goal of halting network operations, potentially causing damage to an organization's reputation, loss in revenue or both.

DDoS attacks continue to escalate, impacting businesses of virtually every size and industry. The number of DDoS incidents reached 7.9 million attacks in the first half of 2023 alone, representing a 31% year-over-year increase.[1]

### How DDoS attacks work

DDoS attacks overwhelm networks with an avalanche of simultaneous requests to slow or halt them. Now, there are greater means to launch strikes, including unsecured, network-connected and mobile devices. Attackers also rely on an ever-evolving repertoire of malware and combinations of DDoS attacks to successfully stage intrusions.

The effect? Whether traffic slows to a crawl or is blocked entirely, customers and employees can't access the information they need, often resulting in a loss of productivity and negative impacts on a company's reputation and bottom line. While a DDoS attack can have a significant financial impact, there are other risks. DDoS threats can often be a precursor to, or distraction from, more serious data breach activity.



Spectrum ENTERPRISE®

### Firewalls are not enough

Traditional firewalls and intrusion prevention systems are often inadequate to defend against today's DDoS attacks, with volumetric attacks being the most common. IT leaders need to quickly detect and defend against these threats to protect their organizations.

### Proactive and protective steps you can take to determine what safeguards to put in place:

**Create** a plan that ensures a fast, comprehensive response, including:

- Support for volumetric/flood attacks.
- Visibility into attacks to help meet regulatory and compliance requirements.

**Design** a customized detection and mitigation strategy to:

- Set up mechanisms to alert for potential threats that enable a quick response to attacks.
- Reroute and scrub traffic at the IP address level, so you can continue to operate without any disruptions caused by malicious traffic.
- Gain 24/7/365 automatic protection and minimize the need for manual intervention to redirect and mitigate malicious traffic.

**Implement** a system to support staff via:

- A managed services partner that provides an always available, single point of contact to engage security experts for swift issue resolution.
- Managed services that help you avoid hiring additional onsite security experts and the need to purchase new equipment.

**Entrust** your internet and network connectivity to a qualified internet service provider (ISP) that can:

- Detect and mitigate DDoS attacks before malicious traffic reaches your network.
- Provide the massive bandwidth capacity best equipped to absorb and disperse large-scale attacks.
- Minimize latency without the need for traffic to be redirected to external scrubbing centers.
- Seamlessly integrate with your existing network infrastructure without the need for you to install or maintain equipment.



Spectrum ENTERPRISE®

### Achieve peace of mind

Find the best protection and mitigation based on your specific needs to keep your customers, your data and your network secure. Below is a list of questions to ask any DDoS protection vendor:

- On what platform is your protection based?
- How do you specifically protect against volumetric DDoS attacks?
- How will you monitor our traffic?
- How do you detect an attack?
- How will you customize protection to address our company's specific needs?
- Can you provide visibility into historical attacks for network planning?
- When can I access support? Tell me about customer service.
- Who do I call when I need help or support?
- What are your support response times?
- How do you differentiate between an intended spike in traffic and an actual attack?

Spectrum Enterprise® DDoS Protection applies adaptive intelligence to quickly evaluate your expected network activity and identify threats. Attack mitigation and traffic rerouting begin automatically to help keep your resources available.

Learn how Spectrum Enterprise can protect your network from DDoS attacks.

1. "Netscout Identified Nearly 7.9 Million DDoS Attacks in 1H2023, According to Its Latest DDoS Threat Intelligence Report," Netscout, September 26, 2023.
2. Ibid.
3. "Global DDoS Summary," Netscout, 2023.
4. Lionel Sujay Vailshery, "Number of Internet of Things (IoT) Connected Devices Worldwide from 2019 to 2023, with Forecasts from 2022 to 2030," Statista, July 27, 2023.

**About Spectrum Enterprise**

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions; Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.





Spectrum ENTERPRISE®