



SOLUTION GUIDE **CHOOSING THE** **RIGHT DDoS SERVICE**

Your guide on what you need to know about DDoS defense, selecting the right solution, and understanding GTT's DDoS Protection and Mitigation Service benefits



CONTENTS

INTRODUCTION	1
THE GROWING DDoS THREAT	2
CHOOSING THE RIGHT DDoS DEFENSE SOLUTION	3
GTT DDoS PROTECTION AND MITIGATION SERVICE	4
THE GTT DDoS DIFFERENCE	5



INTRODUCTION

Distributed Denial of Service (DDoS) attacks are a major cybersecurity threat to an organizations infrastructure. Few providers offer sufficient protection for organizations to defend against these attacks. Those that have implemented protection have a robust defense and are able to effectively keep their infrastructure running while gaining a competitive advantage in the marketplace due to the extra security measures they have taken.

Organizations who are automatically protected against DDoS, in real-time, are differentiating themselves from the competition by prioritizing internet resiliency and their customers' safety.

This guide is designed to help organizations understand the DDoS threat landscape, the right service for them and the value of GTT's DDoS Protection and Mitigation Service.

THE GROWING DDoS THREAT

DDoS attacks continue to rise in size, frequency and complexity, impacting the security and availability of the Internet. The latest breed of multi-vector volumetric DDoS attacks, including flood, reflection, amplification and state-exhaustion, requires mitigation in seconds, not minutes. These increasingly sophisticated cyberthreats have the potential to challenge traditional security defenses and compromise networks.

DDoS attacks have now become an easy method of cyberattack, that just about anyone can launch. The rise of DDoS-for-hire botnets has caused an explosion of attacks, partly due to their cheap price point – they can be launched for just a few dollars – but also because there is virtually no technical barrier to entry because they require zero coding knowledge. While the cost of launching an attack has reduced significantly, the costs incurred by the victims for lost revenue and reputation are increasingly significant. Imagine how many customers an online store could lose if a DDoS attack takes its website offline, for even a few minutes of trading.

Aside from DDoS-for-hire services, Ransom DDoS extortion campaigns have also become a common tool in the cyber-threat arsenal, and one of the easiest ways for an attacker to turn a quick profit. When service availability is threatened, the victim company needs to consider the

potential loss in downtime, revenues and brand damage. When faced with these costly implications, you can understand why some organizations choose to pay the ransom in hope of circumventing an attack. Unfortunately, in most cases, this is futile: the promise of withholding attacks after the payout is often empty.

All of this makes for an extremely concerning future for the DDoS attack landscape. With Ransom DDoS attacks and DDoS-for-hire services evolving so quickly, and the capacity for future botnet-driven DDoS attacks growing incrementally, organizations must stay ahead of the game and take steps to ensure they stay protected. The best way for organizations to mitigate DDoS attacks is to get protected by the latest generation of always-on, real-time, automatic DDoS Protection and Mitigation Service, coupled with the support of expert response teams.

11

**AVERAGE NUMBER OF DDoS
ATTACKS ORGANIZATIONS
FACED PER DAY***

\$1.1M

**AVERAGE COST
OF A DDoS ATTACK***

*Source: 2025 Corero Threat Intelligence Report

*Source: Cyber Management Alliance, January 2025: Recent Cyber Attacks, Data Breaches, Ransomware Attacks

CHOOSING THE RIGHT DDoS DEFENSE SOLUTION

Real-time DDoS protection has become more critical now than ever before. Expectations for Internet response and resilience comes down to seconds, not minutes.

When the Internet goes down, organizations that rely on Internet services go down with it. DDoS attacks are one of the most serious and common threats to business continuity. Downtime and internet disruption can impact brand reputation, customer trust and revenue. To avoid damage to reputation and brand, customers are looking for protection that keeps up with the evolving DDoS threat.

Many commercial solutions are available for organizations to defend against DDoS, but not many of them fully protect against these attacks and prevent the downtime associated with them. Many DDoS mitigation solutions use

legacy approaches and require manual intervention that can take minutes and, sometimes, even tens-of-minutes to block an attack, resulting in downtime for providers and their customers. In addition, organizations need to protect themselves and their customers by offering clean transport, with enhanced security SLAs. When shopping for a DDoS mitigation solution organizations should choose one that protects, not just mitigates attacks, and does so automatically, in real-time, to prevent any possible downtime and maintain business continuity when targeted by an attack.

\$500K-\$5M

**AVERAGE COST
PER HOUR OF
DOWNTIME***

39%

**WEB DDoS ATTACKS
ROSE 39% IN H1 2025 VS.
H2 2024***

50%

**HALF OF DDoS
ATTACKS USE 3+
VECTORS; OVER 50%
USE 2+***

*Source: Erwood Group, The True Costs of Downtime in 2025: A Deep Dive by Business Size and Industry

*Source: Radware H1 2025 Global Threat Analysis

*Source: Astra Security, 2025 DDoS Statistics

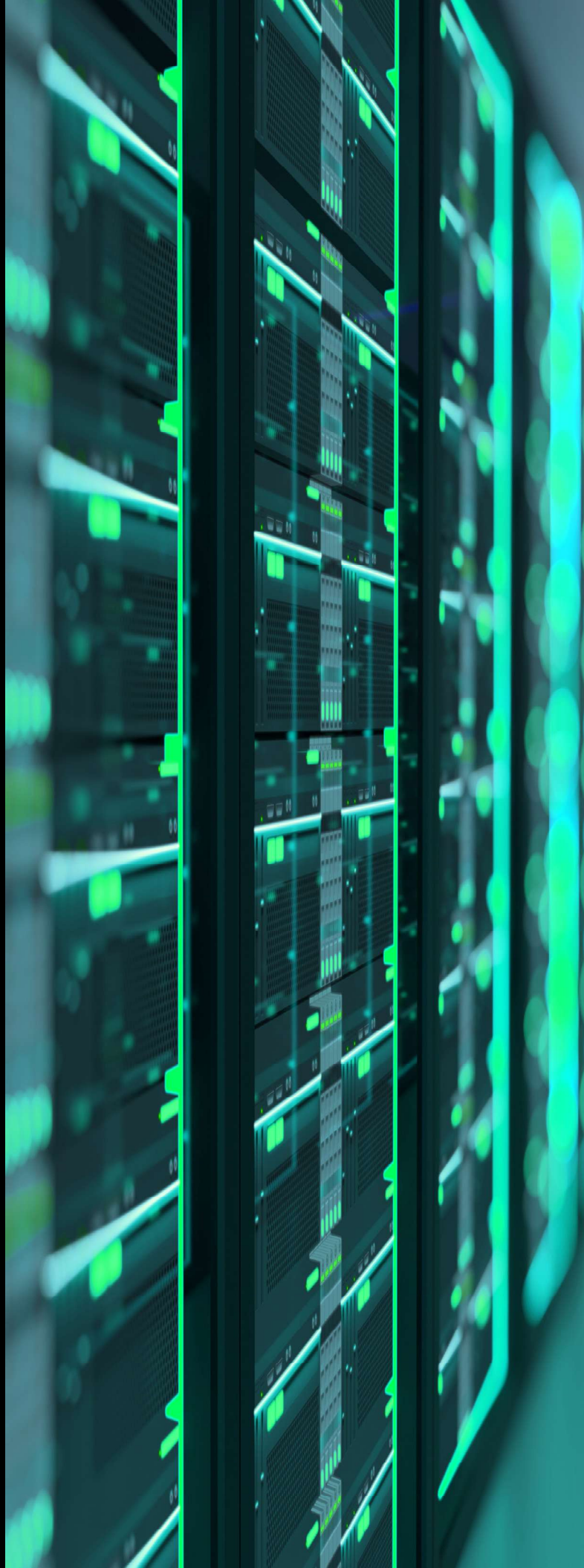
GTT DDoS PROTECTION AND MITIGATION SERVICE

GTT DDoS Protection and Mitigation Service is an innovative solution using real-time, automatic mitigation technology to enable DDoS protection at your full edge bandwidth. We provide the ability to scale to tens-of-terabits where previously only partial scrubbing capacity was feasible.

It's a flexible solution designed for both physical and virtual deployments, as services migrate to support the needs of 5G-enabled environments.

Organizations can take a proactive stance against attacks with GTT's automatic and dynamic DDoS Protection and Mitigation Service capabilities. When under attack, these mechanisms automatically trigger, and operate autonomously. The detection-to-mitigation timeline is reduced to seconds, or even sub-seconds. That's because it eliminates the requirement to manually analyze events, and can avoid the need to reroute traffic (good and bad) in order to remove the DDoS packets.

GTT's DDoS Protection and Mitigation Service automatically blocks over 99% of attacks, eliminating the need for on-site DDoS experts. For cases where further analysis is required to determine if an attack was missed or it was in fact some other traffic anomaly, GTT delivers 24x7x365 support. In fact, 70% of calls are confirmed by our experts as being network issues, not DDoS events - critical information for tracking down true root causes.



THE GTT DDoS DIFFERENCE - PROTECTION WITHOUT THE HASSLE

GTT is here to help you accelerate your security maturity and reduce cyber attacks, saving you time, money and your reputation. Our DDoS Protection and Mitigation Service is not your standard service. We provide even more coverage with our differentiators that include:

LEADING TIER 1 IP NETWORK

Backed by our top ranked global Tier 1 IP backbone providing the capacity and scalability to mitigate large-scale attacks, allowing you to mitigate closer to the source with minimal added latency.

NO LIMITS

It doesn't matter how many IP blocks, # of mitigations, length of mitigations you have, we have you covered.

COMPREHENSIVE SERVICE OPTIONS

Our solution includes multiple service levels and deployment options to fit your organizations needs and budget.

NEXT-GENERATION PLATFORM

Sub-second mitigations compared with much longer detect and divert solutions. Offer better detection than legacy threshold alerting with industry-leading technology.

FLEXIBLE, EASILY DEPLOYED SOLUTION

A no touch, frictionless deployment with a single point of contact and single bill. No complex GRE tunnels, on prem hardware or network configuration changes required.

RESILIENT SYSTEM

Globally geographic redundant scrubbing centers and 24/7 always on protection availability maintained by GTT experts.

Talk to one of our consultants to learn more about our DDoS Protection and Mitigation Service.

**CLICK HERE
TO SPEAK TO OUR CONSULTANTS**

WHY GTT

GTT is a leading networking and security as a service provider for multinational organizations, simply and securely connecting people and machines to data and applications – anywhere in the world. We serve thousands of organizations, bringing together the right people, partners and technology to reduce the burden on IT teams and solve the most pressing networking and security challenges. Built on our top-ranked global Tier 1 network, GTT Envision is a single global technology platform to connect, orchestrate, virtualize and automate enterprise networks, enabling customers with consumable solutions to achieve business missions and meet ongoing demand when, where and how needed. Our portfolio includes SASE, SD-WAN, security, internet, voice and other connectivity options, complemented by a suite of professional services and exceptional sales and support teams in local markets around the globe. We partner with our customers to deliver Greater Technology Together.

For more information, visit gtt.net

