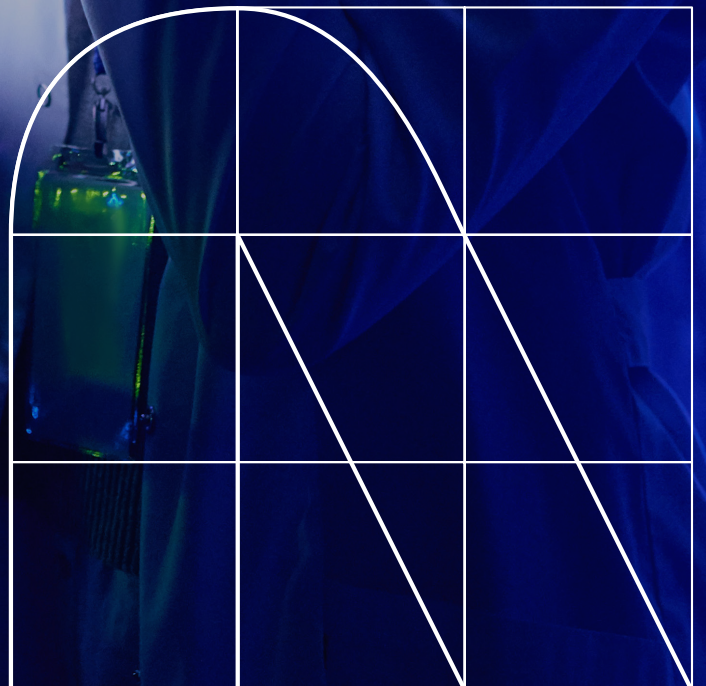


DDoS Protection Services:

DPS Service Provider



A world of cyber insecurity

We are seeing trends such as a record number of consumers accessing the internet for commerce, news and video entertainment as well as the rise of exciting new business areas, such as Artificial Intelligence (AI), Internet of Things (IoT) and virtualization. But a more connected world also means more avenues for criminals to exploit with increasingly sophisticated cyberattacks. Internet-centric businesses and enterprises simply cannot afford to let their guard down, with such breaches having the potential to shut down networks and cost millions. Making protection a central feature when launching new products and services therefore remains a must – and one of the most critical business concerns of the moment.

Distributed denial of service (DDoS) attacks

Core among today's concerns are DDoS attacks, which have become a regular threat to the online business community. These can strike at any time – potentially leading to devastating effects on your network, damaged assets and big revenue losses. And they are growing in size, frequency and complexity – some have compromised hundreds of thousands of devices. Stamping these out before they can create real damage is thus essential.

Volumetric attacks

Volumetric attacks are designed to overwhelm a host or network and make it unreachable. These types of attacks typically come from compromised devices or by the exploitation of certain network protocols, often resulting in some sort of collateral damage and making the network inaccessible to more than just the intended target.

- TCP SYN Flood
- UDP Flood
- ICMP Flood
- Reflection Attack

Application layer attacks

Application layer attacks are well-crafted attacks targeting a specific service on the host. These can be difficult to detect, as they look like a legitimate connection, but are often filled with garbage requests. Due to the numerous tools available, such as the Low Orbit Ion Cannon (LOIC) tool, these attacks have become even more popular among hackers.

- HTTP-GET
- HTTP-POST
- SSL Attacks

State exhaustion attacks

These attacks can be volumetric and/or application layer in nature, often represented by a slowloris attack tool of HTTP-GET or SSL attacks.

A proactive approach to network security

We fully understand the need to keep abreast of these increasingly complex threats. That's why we take a proactive approach to stopping them, not a reactive approach once the damage is already done. Our security products are geared towards supporting multi-threat security environments, and we offer customized options, letting you choose the support that best fits your organization's cyberdefense strategy – for both your organization and your customers.

We also listen to your specific security needs to help you make the best choice. You can rest assured that we have the ideal team to support you: our dedicated Network security team (NST) has an average tenure of 10-plus years, providing truly in-depth expertise. Combined with the backing of our Tier 1 global IP backbone, our security offering is second to none, enabling you to offer a customized and robust DDoS protection to your customers.



DPS service provider

NTT DATA's Global IP Network DPS service provider is a cutting-edge, robust DDoS mitigation service purpose-built for service providers looking to protect their network infrastructure as well as offer enhanced protection to their end-users. As the operator of one of the world's largest Tier 1 Internet backbones, NTT DATA's Global IP Network provides an unparalleled platform that not only shields customer networks against DDoS attacks but also creates an opportunity for customers to build or enhance DDoS protection value-added services for their end-users. By incorporating DPS service provider capabilities into their own services, service providers can enhance their DDoS protection offerings with advanced capabilities and reach, broaden revenue streams and ensure the operational continuity of their end-users.

The DPS service provider service offers an all-encompassing security suite, blending NTT DATA's sophisticated resources, industry-leading DDoS protection technology, and the strategic expertise of our renowned Network security team – the same team tasked with securing the Global IP Network 24/7/365. Utilizing customer-defined and end-user-defined parameters, DPS service provider proactively detects attacks and triggers automatic mitigation, minimizing downtime and maintaining uninterrupted service.

With its robust global coverage, intuitive self-service portal and flexible billing, DPS service provider ensures operational continuity and network resilience against DDoS threats and aligns with service providers' dynamic needs, reinforcing their commitment to excellence in customer experience.





Key features

- DDoS solution that can protect customers and their end-users
- Attack detection and auto-mitigation
- End-user level reporting
- Flexible, usage-based billing model



DPS portal

In the DPS portal, customers can:

- Start and stop mitigations
- View end-user alert activity and mitigation activity
- Provision end-users
- Submit requests for new protection object set ups
- Request changes to ACLs on customer interfaces



Network security team (NST)

Our renowned Network security team is at your service, providing 24/7/365 assistance and expertise in handling complex DDoS attacks.



Service level agreements

ACL changes:

- 1 business day for standard changes
- 30 minutes for emergency changes

Mitigations:

- 15 minutes if initiated by DPS portal
- 30 minutes if initiated by phone, email, or customer portal
- 2 minutes for customer-initiated mitigation using DPS portal
- 2 minutes for auto-mitigation



Global coverage

The Global IP Network's DDoS mitigation platform includes multiple scrubbing facilities strategically located:

- APAC: Hong Kong, Tokyo, Singapore, Sydney
- Europe: Amsterdam, Frankfurt, London
- North America: Ashburn, Los Angeles, Miami, New York, San Jose
- South America: São Paulo

For more information and updates on the Global IP Network:

gin.ntt.net



