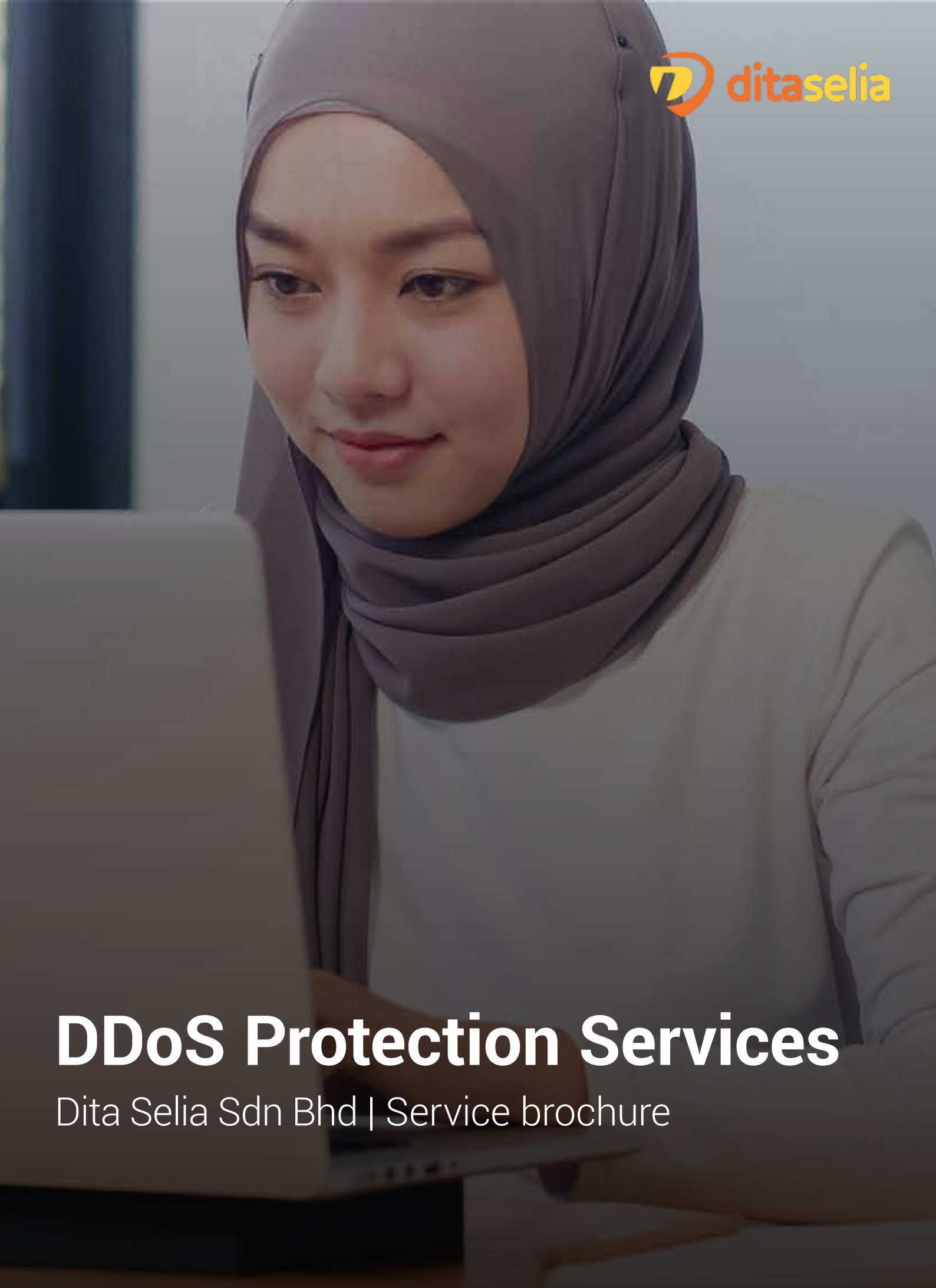

DDoS Protection Services

Dita Selia Sdn Bhd | Service brochure

DDoS Protection Services

A world of cyber insecurity

Record numbers of consumers are going online for commerce, news and video entertainment; the rise of exciting new business areas, such as the Internet of Things (IoT) and virtualization – these are the trends we see today. 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 attack 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.

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.

Dita Selia Sdn Bhd (943657-K)
20-07, Unit 20-07, 20th Floor, Menara K1,
No.1, Lorong 3/137C, Off Jalan Klang Lama,
58000, Kuala Lumpur.

contactus@ditaselia.my
+60 16-330 8032

DDoS Protection Services (DPS)

Our DDoS Protection Services (DPS) offer a comprehensive, tiered approach to DDoS mitigation –depending on the type and level of protection you want. These options give you the chance to get the protection that best fits your defense strategy, whether you want a basic, intermediate or high-level of support. And if you do require strong protection, our services have the capabilities to deal with large-scale attacks, redirecting and cleaning traffic through our mitigation platform. So get in touch with us and defy the criminals before they can deny your service.

DPS Control

DPS Control is our entry-level service. Using this service, customers can define permanent access control lists (ACLs) to block the network from certain types of traffic determined by the customer. So if you do not need full mitigation assistance, but still want a robust service that you can really rely on for basic protection, this could be the option for you. This service offers the following features:

Permanent ACL support

- Supports for ACL up to 50 lines
- Standard and emergency ACL change support

ACL response time service level agreement

- 30 minute response time SLA for emergency ACL requests
- 1 business day response time SLA for standard ACL requests

DPS Core

Our next level of protection is DPS Core. As well as offering a range of extra features, an additional layer of assurance is provided by the support from our Network Security Team (NST) – the very same team that defends our network from attacks. Using state-of-the-art technology in response to a mitigation request, our team can rapidly analyze an attack and take any necessary counter-measures to snuff it out – such as identifying key attack vectors, filtering traffic and rerouting it to our mitigation platform for scrubbing. Get this option if you want a swift, effective response to malicious DDoS activities. In addition to the basic features in DPS Control, this service includes:

Access to Network Security Team

- DPS Core subscribers have direct access to our highly capable Network Security Team, so they can stay up-to-date during mitigations

Mitigation response time SLA

- 15 minute response time for requests via DPS Portal
- 30 minutes for requests via email, phone, or customer portal

Attack mitigation

- Our NST employs a multi-layered approach to attack mitigation and will use a variety of tools and techniques, including scrubbing of attack traffic using our mitigation platform

Portal and reporting

- Our exclusive DPS Portal provides access to mitigation reports and the relevant history

DPS Detect

Want an even higher, more thorough level of support? DPS Detect might be the answer. On top of all the great features offered by DPS Core, it adds services such as detection capabilities to help notify clients of potential attacks, and customer-initiated mitigations at the push of a button from the DPS Portal. Customers can also review their detection history and past mitigation reports, and request configuration changes. So for a full DDoS protection service that covers all the bases, get DPS Detect. The features below are only included in DPS Detect:

Attack detection

- Using customer-defined thresholds, DPS Detect customers will be alerted of potential attacks through the DPS Portal, and optionally by email or syslog

Self-initiated mitigation

- In the DPS Portal, customers can initiate a mitigation based upon an active detection alert, or by specifying the target IP address

DPS Max

The most comprehensive offering for DDoS protection our customers is DPS Max. This service uses a combination of our resources, expertise and mitigation strategies to protect customers affected by DDoS attacks, including attack detection and automatic mitigation. The service is supported by our NST, the same one responsible for defending our network from attacks.

Auto-mitigation

- When notified of a possible DDoS attack, the platform will automatically start a mitigation when an attack is detected, redirecting traffic to our mitigation platform, and stop the mitigation once the attack has ended. No action is needed from the customer

Dita Selia Sdn Bhd (943657-K)
20-07, Unit 20-07, 20th Floor, Menara K1,
No.1, Lorong 3/137C, Off Jalan Klang Lama,
58000, Kuala Lumpur.

contactus@ditaselia.my
+60 16-330 8032