STAND ALONE CLOUD DDoS SOLUTION

VS.

SERVICE PROVIDER DDoS SOLUTION

Comparing multiple DDoS security solutions can be confusing, making it hard to determine which one is right for your business. Besides building out a dedicated solution for your business, there are two major options: stand alone cloud solution or service-provider-based DDoS Protection.

PERFORMANCE

- Provides only DDoS security
- Positioned in front of the ISP causing delayed mitigation

- Provides both the internet connection and DDoS security
- Fast and direct path to mitigate

DETECTION

- Cannot profile traffic without additional resources
- Associated with high infrastructure cost

- Continuous traffic profiling integrated within service to identify traffic trends and attacks with accuracy
- No additional equipment required

ACCURACY

- Cannot redirect individual IPs
- Can only redirect /24 (256 addresses) or more
- Customer is inflicted with “collateral damage” as traffic unaffected by the attack is also redirected

- Mitigation is surgical in its execution
- System can analyze, redirect and scrub individual IPs exclusively
- No "collateral damage" experienced during an attack

DELIVERY

- Uses a GRE Tunnel or a dedicated VLAN for traffic delivery
- Customer is responsible for redistributing traffic delivered across the tunnel to its destination

- Returns clean traffic on existing DIA services
- No GRE Tunnel is required
- Customer is not responsible for redistribution of traffic

Zayo DDoS Protection is comprehensive and precise in its defense compared to stand alone cloud solutions. Zayo is able to profile customer traffic, precisely mitigate attacks and deliver clean traffic with efficiency and ease.

Learn more at **zayo.com/ddosprotection**

zayo