TOP THINGS TO LOOK FOR IN DDoS PROTECTION

Need to protect applications from DDoS attacks? Have applications hosted in a public cloud? In your data-center? Confused by all the options available? This list can help with what is important to look for in DDoS protection for applications.

1. Single solution for applications everywhere: No matter where applications are hosted – on-premise, private or public cloud – look for a unified "single pane-of-glass" solution that can protect your applications anywhere and everywhere.

2. Go for complete coverage: Threats are evolving and massive application-layer and SSL-based DDoS attacks are becoming more common. Chose a solution that offers the widest protection and does not limit to only network-layer attack protection.

3. Do not compromise on quality: Look for solutions that block attacks without impacting legitimate traffic. Solutions that leverage machine-learning and behavioral-based algorithms increase the protection accuracy and minimize false positives.

4. Balance latency with time-to-divert: A hybrid or on-demand cloud service provide the lowest latency. Even for applications hosted on public clouds, look for an on-demand cloud service that still provides real-time protection – it does exist! However, if your applications are attacked frequently, you can save on the constant time-to-diversion by going with an always-on cloud service. In most cases, you'll need a combination of hybrid, on-demand and always-on, to protect different applications depending on where they are hosted.

5. Don't limit mitigation capacity: With IoT botnets resulting in 1Tbps DDoS attacks, you don't want to be limited by your mitigation capacity or pay extra for volumetric attack traffic. Go for a service priced based on legitimate traffic volume and provides unlimited attack traffic capacity as part of that.

6. Keep things flexible: You probably have unique technical and organizational requirements for your network and applications. Choose a service that gives flexible diversion methods - automatic, manual or API-based – so you can chose what works for you.

7. Automation is key: With today's dynamic and automated attacks, you really don't want to depend on manual protection. A service that does not require any customer intervention with a fully automated attack lifecycle - data collection, attack detection, traffic diversion and attack mitigation – will keep you well protected and give you the peace of mind you need.

8. Don't pay more than you need: Avoid hidden traffic costs by going with a full-coverage protection solution, so you don't need to pay cloud providers extra dollars on all the attack traffic that remains undetected and reaches your application.

9. It's not a one-size-fits-all approach: The appropriate deployment – hybrid, on-demand or always-on cloud protection – will vary for each of your applications depending on where the application is hosted (data center, public cloud, etc.) and its sensitivity to delays and latency. Finding the right deployment for each application as part of a single-vendor, holistic solution will introduce efficiencies while still keeping consistency across your DDoS protection.

Don't compromise on DDoS protection for applications. Radware offers the industry's first, fully managed cloud DDoS protection service to protect applications everywhere with integrated, unified protection across data centers and public cloud environments.

Radware is extending its cloud services to offer full network-layer and application-layer DDoS protection for applications hosted on AWS and Azure public clouds with real-time mitigation and no added latency in peacetime. This provides organizations that host their applications on a mix of on-premise and public cloud environments unified DDoS protection with consistent security policy and a single pane-of-glass.