Top Things To Look For in DDoS Protection

Service availability is the cornerstone of the digital experience. Downtime leads to lost revenue, reputational damage and unsatisfied customers. Ensuring service availability by leveraging behavioral-based technologies, understanding the pros and cons of different DDoS deployment options and having the ability to mitigate an array of DDoS attack vectors is now essential.

Here is a checklist of what is important when considering DDoS protection for networks and applications.

1. A Single Security Solution For Applications Hosted In Any Environment

No matter where applications are hosted – on-premise, private or public cloud – look for a unifited solution that provides comprehensive protection for your applications across any environment and from an array of threats.

This should include identifying solutions that provide not only provide core DDoS protection and web application firewall (WAF) capabilities, but also bot management, as many DDoS attacks are now executed via largescale bot networks. These capabilities will provide complete protection, according to Gartner.

Download Gartner's Critical Capabilities for Cloud Web Application and API Protection report to learn more

2. Comprehensive, 360˚ Protection

Per the aforementioned point, threats are evolving and massive application-layer floods and SSL-based DDoS attacks are commonplace. Select a solution that offers the widest protection and is not limited to just network-layer attack protection.

3. Machine Learning Is Critical

Prioritize DDoS mitigation that blocks attacks without impacting legitimate traffic. Solutions that leverage machine-learning and behavioral-based algorithms to understand what constitutes legitimate behavior and automatically blocks malicious attacks are critical. This increases protection accuracy and minimizes false positives.

4. It’s Not A One-Size-Fits All Approach

Flexibility of deployment models is crucial so your organization can tailor its DDoS mitigation service to suit its needs, budget, network topology and threat profile. The appropriate deployment model – 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 and drive consistency across your DDoS protection.

Download Choosing the Right DDoS Solution

5. Balance Latency With Time-To-Divert

Hybrid or on-demand cloud services provide the lowest latency. Even for applications hosted on public clouds, look for an on-demand cloud service that still provides real-time protection. 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 models to protect different applications depending on where they are hosted.

6. Don't Be Limited By Mitigation Capacity

With volumetric attacks now exceeding 5Gbps, ensure you’re not limited by mitigation capacity or have to pay extra for volumetric attack traffic. Ensure any solution you’re considering leverages a pricing model based on legitimated traffic volumes and provides unlimited attack traffic capacity.

7. Granular Service-Level Agreements

DDoS protection is only as good as its SLA. It is the contractual guarantee outlining what your DDoS mitigation provider will deliver and their obligation to remedy in case they do not meet those guarantees.

Ensure any DDoS service includes detailed commitments for time to mitigate, time to detect, time to alert, time to divert, consistency of mitigation and service availability.

Read Six Key Questions To Ask Your DDoS Mitigation Provider

8. Stay 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 choose what works best for your organization.

9. 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.

Cyberthreats are evolving faster than security teams can adapt. Automation improves scalability and minimizes the chances of a data breach.

Download Battling Cyberattacks with Machine Learning and AI

10. Don’t Pay For 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.

Learn More About DDoS
Protection For Any Infrastructure:
On-Premise, Private or Public Clouds