五问您的 DDoS 缓解服务提供商

随着 DDoS 攻击频率和复杂性的加剧，选择合适的 DDoS 缓解服务对于保护您的网络和用户来说至关重要。然而，并非所有服务都能提供同样的防护效果，选错服务可能会导致意想不到的麻烦、性能问题和停机时间。

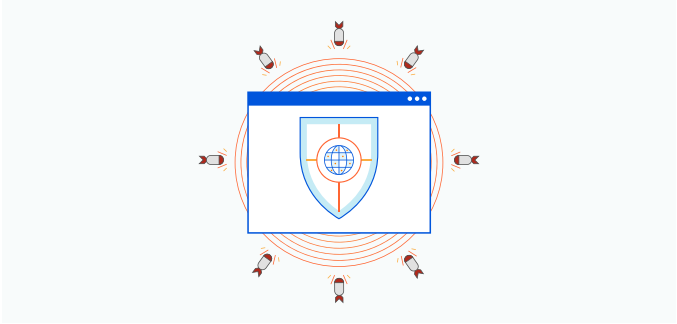
在评估 DDoS 缓解服务提供商时，您应该考虑下面五个问题：

1. 服务是云原生的吗？

DDoS 缓解服务若要发挥效用，必须是云原生的，不能是经过虚拟化并托管在云数据中心的本地部署技术。有何区别？云原生缓解服务可以根据您的业务需求无缝扩展，不会造成人为的性能瓶颈，而云托管虚拟设备仍然具有与本地硬件相关的管理复杂性。

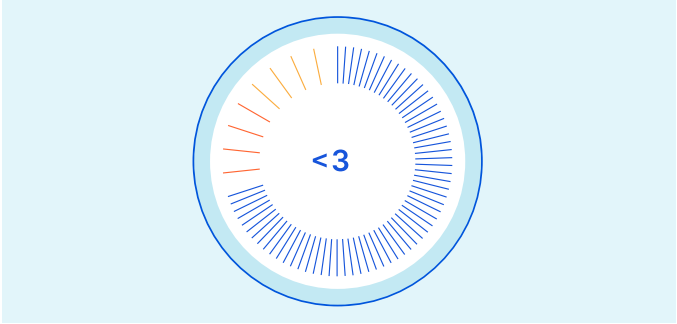
2. 提供商提供的网络容量有多大？

大规模 DDoS 攻击（例如2020 年针对 AWS 客户的 2.3 Tbps 攻击）可能会使网络容量不足的服务提供商不堪重负，无力吸收 DDoS 流量。若要对抗这种规模的攻击，您要选择提供充足网络容量的提供商，从而既能抵御攻击，也不会导致停机或性能下降。



3. 服务可以多快速度检测和响应 DDoS 攻击？

面临攻击时，较短的缓解时间（检测和缓解攻击所需的时间）至关重要。停机时间一旦超过几秒钟，就会给客户体验、品牌声誉和收入造成不可逆转的损害。



4. 服务是否在每个数据中心都可用?

如果做不到 DDoS 清理功能在每个数据中心均可使用，您的流量将不得不通过专门的 “清理中心” 返回，这通常会增加延迟并影响应用程序性能。选择可在每个数据中心提供缓解服务的提供商，同时将您的流量保持在最佳路径上。

5. 服务是自动化的吗?

强大的 DDoS 缓解服务应通过仪表板或 API 提供自动化和自助服务能力，让您能够快速开启和管理威胁防护。您要寻找的提供商必须易于联系，响应快速，主动检测和缓解威胁，并且对您的服务停机时间没有任何影响。

Cloudflare Magic Transit 可保护整个 IP 子网免受 DDoS 攻击，同时还可加速网络流量。Cloudflare 的全球网络（覆盖 200 多个位置的数据中心）每天平均阻止 700 亿次威胁，包括史上规模最大的一些 DDoS 攻击。

要开始使用 Magic Transit，请立即申请免费演示。