MANAGED DDoS SERVICE: WHAT SEPARATES GOOD FROM GREAT?

The case for a managed DDoS protection and mitigation service is well established. Partnering with a provider that can oversee the system's operation takes a big IT issue off your plate, augments your staff resources, and gives you access to specialized DDoS expertise. But not all managed DDoS services are alike. How can you tell a great one from a merely good one? Here are the hallmarks to look for.

FLEXIBILITY TO HANDLE CUSTOM WORKFLOWS

You may already have some operational processes and procedures in place for dealing with DDoS threats. A managed service provider should be able to adapt and align to you, rather than requiring you to change your processes. For example, what is your contact and communication protocol? Under what scenarios do you want the service provider to initiate mitigation action on its own, or seek your authorization? Can the provider support different actions based on different alert types or event levels? A great provider will take the time to understand your processes and have the flexibility to work within them. With many vendors, even good ones, it's their way or no way.

CUSTOMER-FOCUSED REPORTING AND INTELLIGENCE

A good DDoS provider will deliver reports detailing the latest incidents and the actions taken in response to security events. A great one will take a more proactive, consultative approach that leverages global threat intelligence as the basis for recommendations to improve your security posture. A managed service provider should also be able to supply executive-level reporting that enables you to demonstrate ROI and key metrics for the C-suite.

SIZE OF NETWORK

DDoS attacks are growing in sheer size and rapidly approaching terabyte territory, due largely to amplification techniques and the emergence of Internet of Things (IoT) botnets. The capacity to absorb and disperse the largest known attacks is simply a must. Equally important is a distributed infrastructure, with multiple locations that enables mitigation to take place as close to the source of attack as possible. This not only avoids "choke points" — it accelerates time-tomitigation cycles.

While absolute network size is an important consideration, so too is the amount of capacity dedicated to DDoS mitigation. For instance, some content delivery networks and web service providers, that boast enormous network capacity, may offer DDoS protection as a sideline. But it only stands to reason that they will dedicate most of their network capacity to their main line of business, leaving their DDoS customers at risk.

That's why a dedicated provider is critical to mitigating massive attacks. Having said that, managed service providers support multiple customers, and there is always the risk that several will be hit at once. It is not enough, therefore, to have capacity levels that are equal to or even twice the size of any potential attack. Rather, the network must be several orders of magnitude larger than the largest known attacks. Ten terabytes of capacity is quickly becoming the standard that will define the modern, managed DDoS provider.

EXPERIENCE OF TEAM

A good provider will be highly reliant on automation. Certainly, automation plays an important role in effective DDoS protection, but it can't always distinguish good traffic from bad. Left unchecked it is likely to block legitimate traffic and generate a lot of false positives. Thwarting nefarious actors takes human intelligence – the ability to recognize and analyze a real attack, understand its origins and quickly determine its objectives. A great provider will have dedicated research teams with decades of experience studying, analyzing and overseeing the successful mitigation of DDoS attacks. And it will have a deep bench of security expertise with diverse professional backgrounds and complementary skills.

BEST-PRACTICE HYBRID SOLUTION

Many managed service offerings are entirely cloud based. That means 100% of mitigation takes place in an "always on" cloud-based system, which can quickly get expensive. Increasingly, security experts agree that a hybrid solution, combining on-premise and cloud capabilities, is the best defense against DDoS attacks. The on-premise component can typically capture the vast majority of malicious traffic. If an attack threatens to exhaust the capacity of an on-premise appliance, the cloud capability can automatically activate.

What's more, a hybrid solution is less expensive and a better value than you might think. These days, on-premise defenses can be virtualized. With a fully managed service, costs are offset by a reduction in staffing requirements. And you only pay for as much cloud capacity you consume.

When you add it all up, why settle for good?

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SECA_007_EN-1801 08/2018