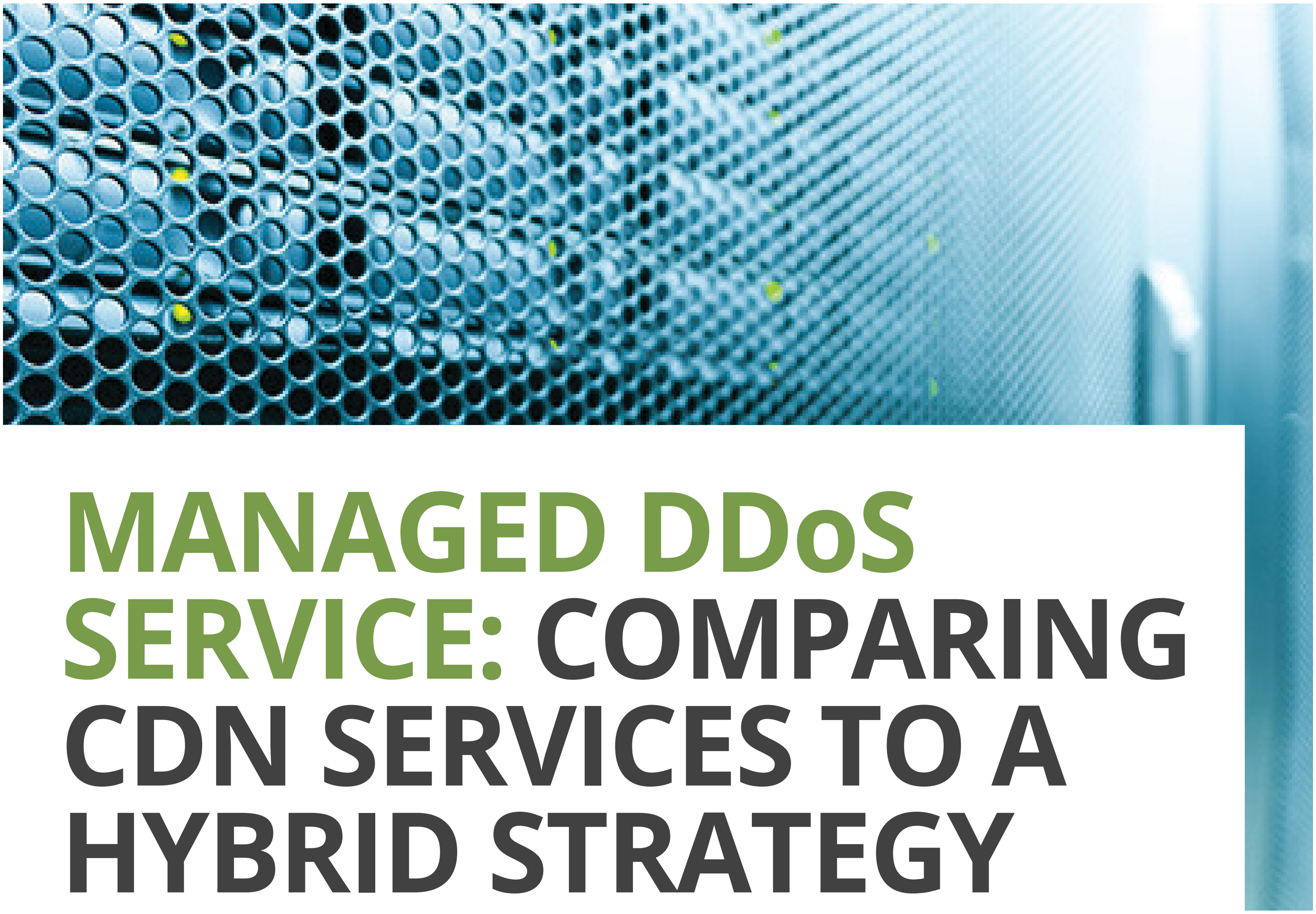

MANAGED DDoS SERVICE: COMPARING CDN SERVICES TO A HYBRID STRATEGY

Among the options available for protection against DDoS attacks, some enterprises turn to content delivery networks or CDNs – globally distributed networks serving web content such as streaming video to end users.

Being distributed in nature and having bandwidth to spare, some CDNs offer DDoS protection for the services they host as well as for service providers (ISPs) and enterprises outside their networks. While this may be a viable option in some cases, or as part of a broader multi-layered protection strategy, companies considering CDNs should be aware of their drawbacks compared to a dedicated, managed DDoS service.

For one thing, security is not a CDN provider's primary focus. Its core business is content and application delivery. Attack investigation, development of countermeasures and threat intelligence are at best secondary considerations. Moreover, CDN providers may lack the resident expertise to research, analyze and understand the nature of attacks, and make informed recommendations to bolster security.

Understandably, a CDN's first protection priority will be the services it is hosting. In the event of an overwhelming, super-sized attack – the kind that is occurring more and more these days – a CDN may not have the capacity to protect all its customers' assets and is bound to leave some exposed. CDN automated countermeasures are also known to block legitimate traffic at times. And because CDN mitigation strategies frequently utilize static filters and web application firewalls (WAFs), they may lack flexibility and intelligence in protecting cloud-based services.

"ALWAYS ON" IS NOT ALWAYS GOOD

CDNs promise "always on" protection, which sounds good but raises some issues on closer inspection. "Always on" can mean one of two things: either traffic is constantly going through mitigation systems that actively inspect and automatically trigger blockage ("always mitigated"), or traffic is simply monitored and passively inspected in order to detect possible attacks and activate mitigation actions on-demand ("always monitored"). It's important to understand the distinction and which one the provider is delivering.

If it's "always mitigated," you need to assess the balance between maximum mitigation of attacks and minimum impact on legitimate traffic. False positives are not the only possible collateral damage of always-on mitigation. Services can be delayed by unnecessary traffic inspection. In the case of "always monitored," you risk losing visibility into attack detection policies and reaction times. You might avoid unnecessary mitigation but, on the flip side, miss relevant attack indicators. Moreover, an always-on solution designed to detect volumetric attacks is likely to miss application layer attacks, which are smaller in scale.

"Always on" protection models require complex traffic balancing in order to mitigate DDoS attacks while preserving normal operations for all customers. This is not trivial, given the large scale of attacks recently observed, and might result in either mitigation impact on non-attacked customers or in the segregation of attacked customers into sub-sets of the total CDN capacity. Customers should carefully assess whether an always-on provider has the scalable architecture to mitigate attacks on some customers without affecting others.

A HYBRID SOLUTION

Increasingly, industry analysts and experts are pointing to hybrid security solutions as best-practice DDoS protection. A hybrid strategy combines an always-on on-premise, dedicated detection and mitigation system with on-demand cloud-based mitigation capabilities. Most attacks are still small enough to be detected and mitigated locally. A local appliance will also be more familiar with application traffic than a CDN solution, and therefore better able to recognize anomalies in traffic patterns. Cloud-based mitigation is automatically triggered only when an attack clearly exceeds the capacity of the on-premise unit. Accordingly, there is no reason for the cloud component to be "always on," saving on costs and conserving capacity to fight actual attacks.

Cost may be one of the key drivers to CDN DDoS providers. However, a hybrid solution can be surprisingly economical. Virtualization technology can replace expensive hardware. And when deployed as a fully managed service, backed by DDoS experts, the costs of a hybrid solution can be offset by a reduced internal IT footprint and security staffing needs.

Finally, a CDN solution typically relies heavily on automation. Attackers today are cunning and creative. While automated detection and mitigation capabilities are absolutely essential, thwarting attacks also requires a team of people with the experience, training to outthink and outsmart malicious actors. A powerful threat intelligence network and deep research program will multiply the effectiveness of a hybrid technology solution many times over – strengths you are more likely to find with a dedicated DDoS security specialist than at a typical CDN provider, where security is a sideline.

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.

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