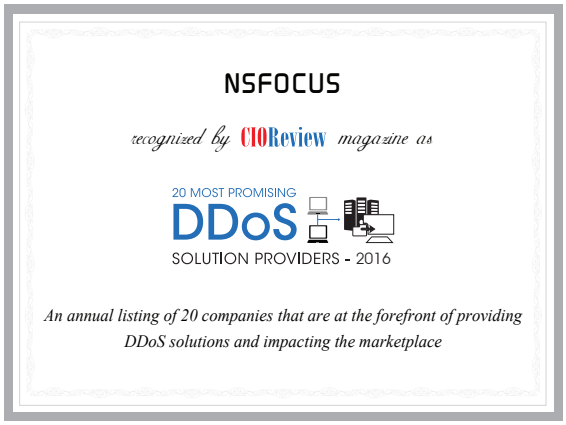
CIOReview
The Navigator for Enterprise Solutions
DDOS SPECIAL NOVEMBER 28, 2016 CIOREVIEW.COM

20 Most Promising DDoS Solution Providers 2016

The corporate world is constantly getting smarter by leveraging the latest internet technology advancements. Information sharing has over the years witnessed a gradual displacement of paper with digital becoming the dominant and favored medium. While, undeniably, this transition has boosted communications within and between enterprises, it has also made it a lot easier for hackers to breach an enterprise and disrupt these communications, curtailing business operations. Attackers infiltrate an enterprise's Domain Name System (DNS)—freezing the network or infecting the DNS with botnets.

Such infiltrations, known as Distributed Denial of Service (DDoS) attacks, make business operations arduous by temporarily suspending services and making them unavailable for customers. To purge these challenges, it becomes important to defend an enterprise's DNS servers and networks from DDoS onslaughts. Preventing these infiltrations requires purpose-built network architecture which can detect and subdue the often deceptive and wildly complex DDoS attacks.

In the current IT market sphere there are many DDoS solution providers offering secured services with a myriad of features and functionalities—Software-as-a-Service (SaaS), traffic control, and firewall protection to fight DDoS attacks in different layers. Presently there are vendors providing solutions that can curb attacks of up to 300Gbps, and above. CIOReview helps enterprise CIOs looking for key technologies related to DDoS navigate this landscape by presenting a list of '20 Most Promising DDoS Solution Providers 2016.'



Company:
NSFocus

Description:
The company offers industry-leading solutions for anti-DDoS, web security, and enterprise-level network security

Key Person:
Stephen Gates,
Chief Research Intelligence Analyst

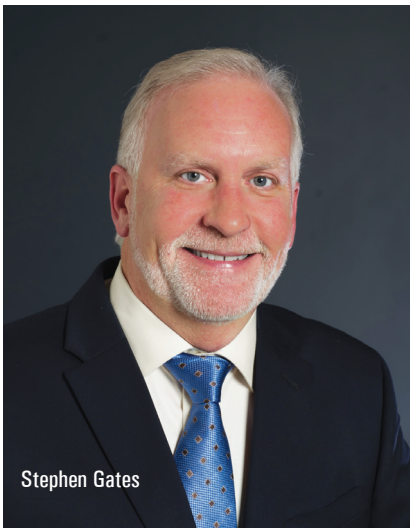
Website:
nsfocusglobal.com

NSFOCUS
Outage or Breach—Pick your Poison

Distributed Denial of Service (DDoS) attacks and network breaches have escalated across many industries owing to the increasing arsenal of automated tools used by cybercriminals. This has put companies in a dangerous position. "Often organizations fail to identify suspicious traffic on their network until it's too late," explains Stephen Gates, Chief Research Intelligence Analyst, NSFOCUS. As a result, companies are looking for ways to identify and eliminate unwanted malicious traffic while not disrupting legitimate traffic. NSFOCUS addresses this quandary, by providing DDoS protection solutions that inspect network traffic, detect DDoS attacks, and mitigate them without affecting legitimate traffic. "We use a combination of algorithmic, signature, and behavioral detection techniques for advanced DDoS protection," explains Gates.

"Organizations can deploy NSFOCUS DDoS protection as an on-premises solution, Anti-DDoS System (ADS), or subscribe to the company's cloud solution," states Gates. Once NSFOCUS' ADS is deployed, organizations can monitor traffic in real-time with a complete suite of IP protocols to ensure network visibility. This allows them to identify and quickly mitigate malicious traffic through NSFOCUS' multi-stage detection engine.

For larger enterprises and service providers, the company's cloud solution, DDoS Protection Service (DPS) uses Border Gateway Protocol (BGP) diversion for redirecting incoming traffic to NSFOCUS Cloud Centers. "The NSFOCUS Cloud is made up of seven cloud centers that are strategically located where vast amounts of internet traffic originates and terminates with the largest Internet exchanges," explains Gates. The


Stephen Gates

cloud centers remove unwanted traffic and send the clean traffic back to the customer. The service can be deployed either on-demand or as always-on protection.

Additionally, clients can utilize a hybrid anti-DDoS approach by combining NSFOCUS' on-premises defenses with on-demand Cloud DPS. This eliminates smaller attacks on premises, while defending infrastructures against larger DDoS attacks using the cloud solution. Alongside DDoS protection solutions, NSFOCUS delivers comprehensive threat protection through a Next Generation Intrusion Prevention System (NGIPS). "Our NGIPS combined with NSFOCUS Threat Analysis System (TAS) is designed to defeat known, as well as unknown malware in clients' networks," says Gates.

All of the company's technologies and solutions integrate with NSFOCUS Threat Intelligence (TI) Subscription Service, providing clients with actionable intelligence that minimizes risk and improves overall security posture. "We recommend the intelligent hybrid security approach that comprises real-time threat intelligence, cloud-based services, and on premises technologies, enabling customers to take threat intelligence and put it into action," describes Gates. The company has empowered thousands of clients with threat intelligence and protection services. For instance, Micron21, a web hosting and data center provider, received complaints from their customers who were experiencing minor DDoS attacks that took them offline. Micron21 sought help from NSFOCUS, and implemented the ADS. "The client quickly mitigated the DDoS attacks, enhancing the reliability of their offerings," says Gates. Micron21 also introduced DDoS-as-a-Service to their customers, starting with a single NSFOCUS ADS deployment that has grown to five geographically-diverse DDoS clustered scrubbing centers worldwide.

> **"Organizations can deploy NSFOCUS DDoS protection as an on-premises solution, Anti-DDoS System (ADS), or subscribe to the company's cloud solution**

This year, NSFOCUS has expanded its footprint beyond Asia-Pacific, by entering new markets in North America, Middle East, and Europe. NSFOCUS is bringing several advancements to its technologies in the coming years. The company will deliver security automation, develop engines that are capable of machine learning, and incorporate artificial intelligence to protect organizations from evolving network breaches. CR