Under attack now? Call +1-855-727-1209.

We can mitigate in just minutes!

Protect your business, protect your brand with intelligent DDoS protection

Need more information?

CONTACT US TODAY!

DDoS is More than Bits and Bytes, It's an Attack on Your Business

Distributed denial of service (DDoS) attacks target important computing resources, such as servers, websites, and applications to cause disruptions in your business. Often, attackers assemble botnets–networks of infected computers–to generate the traffic to paralyze a site. When the targeted server receives too many information requests, the main system crashes.

Bottom line: customers are blocked from reaching your site. Your online business grinds to a halt and your brand takes a hit.

Neustar SiteProtect: Intelligent DDoS Protection for Business

DDoS attacks pose a continuous risk to your website and profits. It's no longer a matter of whether an attack will occur, but rather when and how often.

Neustar SiteProtect is a purpose-built, anti-DDoS protection solution that offers deployment options to fit the needs of all businesses, whether on premise or in the cloud. With a 1:1 scrubbing capacity, SiteProtect defuses complex attacks that threaten your website and business stability. With the right blend of expertise to anticipate DDoS attacks, and the technology to stop them, Neustar keeps your website up when the bad guys try to knock it down.

Neustar SiteProtect offers two types of DDoS protection: on-demand and hybrid.

On-demand DDoS protection

SiteProtect is a high-capacity, cloud-based DDoS protection service that scrubs malicious traffic away from your infrastructure. Your traffic is redirected to a cloud-based "scrubbing" center, where security engineers with years of DDoS experience employ diverse technologies and proven attack responses. The on-demand protection that SiteProtect affords can be activated through DNS redirection or BGP redirection.

Learn More about DDoS Mitigation Options

Neustar SiteProtect: Always-On Hybrid DDoS Protection

Top analysts agree: hybrid DDoS protection is the strongest you can deploy. It combines always-on hardware to block attacks, with cloud-based mitigation to handle larger incidents.

Neustar SiteProtect Hybrid features the best-in-breed Arbor Pravail® DDoS mitigation appliance, which rapidly combats attacks locally. When attacks exceed local capacity, Neustar fails over your traffic to the SiteProtect cloud and mitigates the attack.

SiteProtect Hybrid is a fully managed service, including remote management of your Arbor Networks hardware appliance. Neustar monitors, detects and responds to DDoS attacks for you, so you can commit resources to higher priorities.

DDoS Attacks Are Growing, But Your Resources Are Not

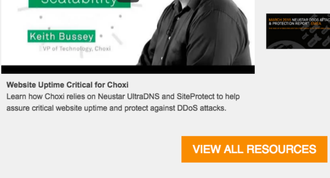
They're real: DDoS attacks are a nuisance; something you wish would just go away. You have better things to deal with, not to mention finite resources. But if an attack takes you offline for a day, the nuisance becomes a menace. And if it's really a smokescreen for other threats – theft of customer data, intellectual property or funds – you need to be prepared. Until now, there were two options – hardware or cloud.

Hardware alone defenses: On-premise hardware is always on and lets you respond immediately. However, you have to dedicate resources to manage the equipment and that is no easy task. Also, hardware can be overwhelmed and leave your organization vulnerable to large attacks. In an age where 100Gbps attacks no longer raise eyebrows, it doesn't take long for your local protection to reach its breaking point.

Cloud defenses: Solutions from cloud providers, like Neustar, offer greater bandwidth, diversity in hardware to mitigate all types of attacks and the 24/7 expertise of trained DDoS fighters. These services are provided on demand. Either can be a strong option, depending on your needs, though managing the hardware or detecting the attack falls on you: one more thing for your hard-pressed staff and budget to absorb.

Best-of-Both-Worlds: On-Premise Box + Cloud, All Fully Managed

To both mitigate instantly and escalate as needed, security experts recommend a hybrid approach, combining the best of on-premise hardware and cloud-based solutions. Neustar SiteProtect Hybrid DDoS Protection is exactly that and more. The service features the best-in-breed Arbor Pravail® DDoS mitigation appliance, which combats attacks locally, without a moment's delay. When attacks exceed local capacity, Neustar fails over your traffic to the SiteProtect cloud and manages the response until the danger passes. Best of all, it is a fully managed service, including remote management of your Arbor box. Neustar monitors, detects and responds to DDoS attacks for you, so you can commit resources to higher priorities.



Using on-premise DDoS hardware plus Neustar's expertise and cloud-based mitigation:

- **Reduce Downtime** – On-premise hardware acts immediately and automatically to mitigate attacks. Managed cloud failover minimizes the risk of larger attacks crippling your site or applications.
- **Protect Against All Attacks** – Some solutions only mitigate certain types of attacks. Blending equipment from Arbor Networks and other top providers, SiteProtect Hybrid defends against attacks across your entire web infrastructure.
- **Stay Focused On Core Objectives** – DDoS attacks are designed to throw your business off track, including valuable IT resources. With our managed solution, we take care of attacks so you can take care of business.
- **Leverage Deep Expertise** – The experts at the Neustar Security Operations Centers average 10 years of experience in DDoS mitigation.
- **Rely On A Single Point Of Contact** – Our managed service simplifies your DDoS responses. Count on Neustar before, during and after DDoS attacks for downstream and upstream protection, plus peace of mind.
- **Gain A Best-in-Breed Solution** – Industry-leading Arbor equipment plus Neustar cloud service equal the strongest mitigation solution you can get.

DDoS Attack Types: Three of the Most Popular

Network attacks: These attacks clog the pipelines connecting your network, website, or online service to the Internet. Because network attacks generate such huge amounts of traffic, they're also known as volumetric attacks. With the availability of cloud-based computing, and the infrastructure to support it, network attacks are growing in size, with some topping 200-300 Gbps.

Protocol attacks: This type of attack is engineered to exploit network protocols—for instance, network time protocol (NTP), which syncs time between machines on any given network. When configuring network protocols most people "set it and forget it." There are few security updates, leaving exposure to risk. Unlike volumetric attacks, protocol attacks are measured in velocity, in packets per second (PPS), as opposed to bandwidth.

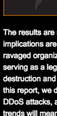
Application attacks: Here, the attacker overloads the resources behind a website application, such as the search function or email service, versus attacking the whole network. Often disguised as legitimate traffic, these surgical strikes are large enough to crash most mid-sized sites, or disrupt larger ones enough to make customers notice.

Complexity and aggression mark the DDoS attacks of the modern assault. Attackers use many variances and combinations of attacks together to achieve desired impacts. Here are just some attack examples of what can be levied against your business:

- TCP SYN Flood
- DNS and exploitation of DNSSEC
- NTP reflection
- UDP/SSDP reflections and floods
- Slowloris
- ICMP (Ping of Death)
- SUNPRC
- NetBIOS
- Portmapper
- SNMP amplification
- HTTP Flood
- NXDomain
- Mixed SYN + UDP or ICMP + UDP Flood
- Chargen
- Smurf

Warning: Many attacks today employ more than one method. By mixing things up and confusing defenders, attackers raise their odds of success.

Arm Yourself with New Research on DDoS Threats



The results are staggering. The implications are severe. DDoS attacks ravaged organizations across the globe, serving as a legitimized weapon of destruction and extortion instrument. In this report, we detail the current state of DDoS attacks, and examine what these trends will mean for IoT.

First Name: *

Last Name: *

Email Address *

Job Title: *

Company Name: *

DOWNLOAD NOW

With Neustar SiteProtect, your organization has access to the people, processes, and technologies that help you:

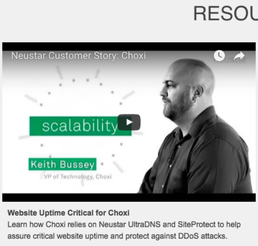
- Protect revenue flow by keeping your business online
- Reduce costs and risks associated with DDoS attacks
- Keep promises to customer and partners
- Maximize budgets to align with strategies
- Reduce the complexity and risks of DDoS defenses

SiteProtect Specs

- Massive 1:1 network to scrubbing capacity
- Expertise and deep experience mitigating Layers 3, 4, and 7 attacks
- Proven processes from 10+ years of anti-DDoS protection experience
- Fast, easy deployment and mitigation
- Flexible options to suit strategies, needs, and budgets

For the complete specification read the product overview

RESOURCES



Website Uptime Critical for Choxi
Learn how Choxi relies on Neustar UltraDNS and SiteProtect to help assure critical website uptime and protect against DDoS attacks.

US DDoS Attacks and Protection Report 2015

Download this report to get a broad perspective on DDoS trends in the U.S. Being fully informed is the first step towards minimizing your vulnerability. Read More

EMEA DDoS Attacks and Protection Report 2015

Download this report to get a broad perspective on DDoS trends in EMEA. Being fully informed is the first step towards minimizing your vulnerability. Read More

VIEW ALL RESOURCES