DDoS Mitigation Services

Comparing NexusGuard and Prolexic

It's not easy being the industry leader. Competitors are constantly snapping at your heels, attempting to convince potential customers they are more cost effective or have better – or at least equal – capabilities. While we welcome competition, we want to be sure you understand the differences between NexusGuard and Prolexic. And despite what you may have been told, there are real tangible differences. Some may seem minor now, but it's the little details that will make a huge impact on your business and web site availability when you are experiencing a Distributed Denial of Service (DDoS) attack.

This "cheat sheet" can help you compare the facts about Prolexic and NexusGuard so you know what level of service you are buying. Despite what you are being told by other vendors, when it comes to mitigating the largest, most complex DDoS attacks, there really is no comparison to Prolexic's capabilities and track record.

Criteria	Prolexic	NexusGuard
Ownership	Prolexic's major shareholder is a leading Silicon Valley equity investment firm called Kennet Partners (www.kennet.com).	NexusGuard is owned by operators of an Asian online gaming and gambling business including Philippines-based Caspo, Inc. Limited company information is available.
Experience	Prolexic has been 100% focused on DDoS mitigation since 2003. In the world of DDoS mitigation, experience is everything.	NexusGuard was incorporated in 2008 and is a relatively new entrant into the DDoS mitigation field.
Infrastructure – bandwidth	Prolexic has over 375 Gbps of bandwidth distributed around the world and 100% of it is dedicated to DDoS attack traffic.	NexusGuard has nowhere near the dedicated DDoS attack mitigating bandwidth that Prolexic has.
Infrastructure – network architecture	Prolexic currently has four global scrubbing centers located in London, Hong Kong, Virginia and San Jose. These are equipped in parallel – as redundant centers – with the same equipment capable of mitigating all types of DDoS attacks.	The vast majority of NexusGuard's mitigation resources reside in Asia. This makes it relatively simple for attackers to overwhelm its other scrubbing centers with DDoS traffic. When they go down, the Asian scrubbing center will have to support NexusGuard's entire client base and all attack traffic. With far less bandwidth than Prolexic, this is just not possible and will lead to outages and possibly blackholing of traffic.
Infrastructure – carriers	Prolexic selects carriers based on quality of service and capacity, not price. Prolexic uses the same three Tier-1 global carriers in all scrubbing centers so it can effectively manage high volume attacks by balancing traffic globally without manual intervention. Prolexic has canceled contracts with many of the providers that NexusGuard currently uses because they could not provide the contracted bandwidth.	NexusGuard primarily uses Tier-2 and Tier-3 carriers. As NexusGuard is not using the same carriers across all of its datacenters it is not able to balance traffic easily, resulting in suboptimal routing and outages due to link saturation. NexusGuard's choice of carriers indicates they have been selected based on price, not quality of service.

PROLEXIC
DDoS Attacks End Here.

Criteria	Prolexic	NexusGuard
Infrastructure – AS path lengths	Because Prolexic only uses a few Tier-1 carriers, traffic latency is minimized and high reliability is ensured.	Traffic has to cross many more networks to reach a NexusGuard customer. Compared to Prolexic, latency is going to be higher simply because traffic has to stay on the Internet longer before it reaches the NexusGuard network. It also means that as there are more third parties involved in the traffic path, more things can go wrong to interrupt that traffic.
Attack volume	Prolexic handles thousands of attacks each year – far more than any other provider. In addition, because of our large, globally diverse client base, we also fight the biggest and most complex attacks. Prolexic regularly mitigates attacks over 25 Gbps.	NexusGuard sees a fraction of the attack volume that Prolexic sees. That's critical, because in DDoS mitigation, experience and bandwidth is everything. Ask NexusGuard to provide documentation of the largest attacks it has successfully mitigated and compare to Prolexic.
Layer 7 attacks	Prolexic has developed its own hardware, proprietary software, and processes to effectively mitigate Layer 7 attacks.	Ask NexusGuard how it detects and mitigates application layer (Layer 7) attacks. Ask how it handles a live hacker that changes tactics during a Layer 7 DDoS attack.
Randomized GET Flood mitigation capabilities	Prolexic is the only provider able to mitigate and clean SSL post and GET Flood attacks.	Ask NexusGuard to demonstrate its pattern matching and "on the fly" signature creation capabilities.
Time to mitigate guarantee	Prolexic's time to mitigate is the fastest in the industry. In fact, Prolexic was the first company to integrate a "Time to Mitigate" (TTM) SLA into its contract language (2010). A Level 1 Prolexic technician based at our Security Operations Center can handle all customer attacks without escalation. This results in a rapid and focused response.	Ask NexusGuard for a time to mitigate SLA and read the fine print.
Mission critical client base	Prolexic's client base features global businesses with mission critical Internet facing infrastructures, including 6 of the world's 10 largest banks.	Ask NexusGuard for a list of its DDoS clients and compare. See how many have mission-critical infrastructures in at-risk industries like e-Commerce and financial services.
Security Operations Center	Prolexic has a full-time staff dedicated to providing first-line mitigation services 24/7.	Ask NexusGuard how many full-time mitigation staff it has and ask to tour its operations center and compare to Prolexic.
PCI compliance	Prolexic is the first DDoS mitigation provider to secure PCI DSS (Payment Card Industry Data Security Standard) level 1 certification.	NexusGuard is not PCI DSS certified for DDoS mitigation. If your industry requires certification, it will take time and cost money to audit NexusGuard.

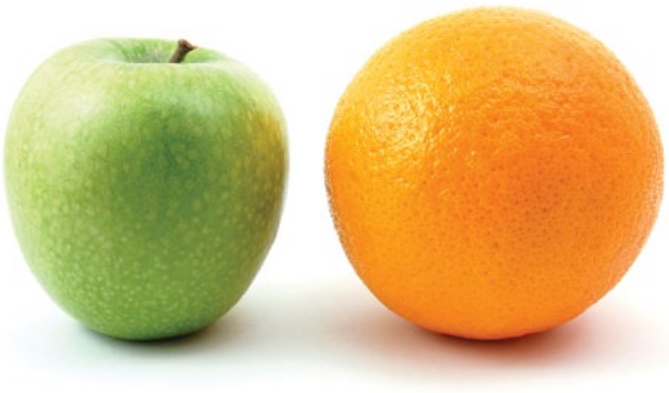
It's a fact. Prolexic represents the gold standard for DDoS mitigation. While others claim to do what we do, when you look closely it's not even close. The simple truth is that in an industry of "me-too" providers making big promises, Prolexic stands alone as the world's first, largest and most trusted DDoS mitigation provider with unmatched experience, expertise and resources.

About Prolexic

Prolexic is the world's largest, most trusted distributed denial of service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Fourteen of the world's twenty largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit **www.prolexic.com**, email **sales@prolexic.com** or call **+1 (954) 620 6002**.

v.02-29-12

PROLEXIC
DDoS Attacks End Here.



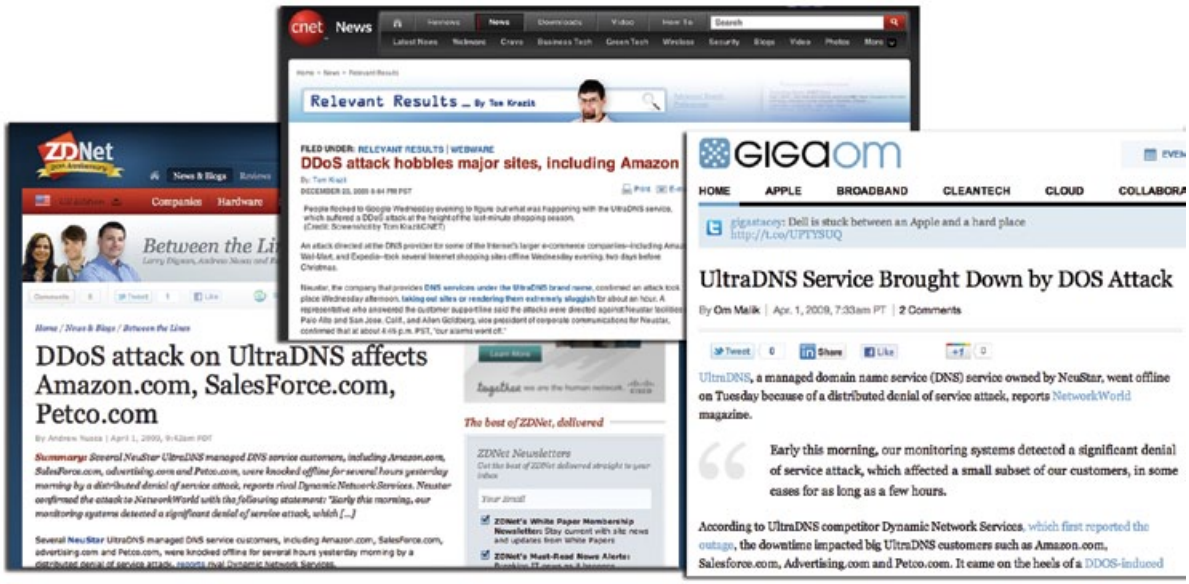
DDoS Mitigation Services

Comparing Neustar & Prolexic

Competition is healthy. We welcome it. But here's the problem. When others start making big promises – claiming their services and resources are a match for ours, but for significantly lower cost – it makes your task of vendor selection more difficult and more confusing.

With your web site, reputation and brand equity on the line you cannot afford to make the wrong choice. And that means choosing a mitigation provider that can guarantee 100% success at overcoming ALL DDoS attacks. And that provider is definitely not Neustar, it's Prolexic.

But don't just take our word for it. There have been many articles in the media about how Neustar's UltraDNS managed DNS service has been affected by DDoS attacks. This has impacted the web sites of major companies like Amazon, Wal-Mart and Expedia – one event occurred during the year's busiest shopping period, just two days before Christmas[1]. Just imagine if that happens to your web site. If Neustar cannot protect its own services against DDoS attacks, do you really want to trust them with your web site?



Neustar's failures to protect its own UltraDNS managed DNS services from DDoS attacks are well documented

If you need more reasons to choose Prolexic, we've provided the following "cheat sheet" to help you compare the real facts about Prolexic and Neustar so you know exactly what level of protection you are buying. Once you do that, you'll see it really is like comparing apples and oranges. Despite what Neustar claims, we are two very different companies offering two very different levels of protection.

PROLEXIC
DDoS Attacks End Here.

Criteria	Prolexic	Neustar
Success rate	Prolexic has never failed to mitigate a DDoS attack – and we have handled the largest, most complex attacks ever launched.	Neustar's failures to protect its own UltraDNS managed DNS services from DDoS attacks are well documented.
Business focus	Prolexic has been 100% focused on DDoS mitigation since 2003. That's all we do.	Neustar's core business is DNS services. It is a relatively new player in DDoS mitigation.
DDoS Investment	Last year Prolexic invested US$15 million back into the business and 100% of that was dedicated to DDoS mitigation.	Ask Neustar how much it invested last year in resources dedicated 100% to DDoS mitigation.
Infrastructure – Scrubbing Centers	Prolexic currently has four global scrubbing centers located in London, Hong Kong, Miami and San Jose. Each scrubbing center is 100% dedicated to handing attack traffic. Prolexic's scrubbing centers are equipped in parallel – as redundant centers – with equipment capable of mitigating all types of DDoS attacks.	Neustar has 15-node global IP Anycasted scrubbing centers. While that sounds impressive, Neustar uses this same infrastructure to support DNS services, which is its core business. What happens when a large DDOS attack starts to overwhelm this network? It's likely that Neustar will protect its core business and DNS customers – some of the largest networks on the Internet – by "blackholing" DDoS attack traffic which will take down your site. Is that what you signed up for?
Infrastructure – Bandwidth	Prolexic has more than 375 Gbps of bandwidth and 100% of it is dedicated to DDoS attack traffic. No one comes close to matching this.	Neustar has a 130 Gbps network divided among 15 sites – that's an average of less than 10 Gbps per site. Prolexic routinely sees attacks bigger than 10 Gbps from a single region so Neustar will struggle by distributing bandwidth so broadly.
Infrastructure – Network Architecture	Prolexic's network is built around four scrubbing centers with extremely high bandwidth in each center.	By having so many scrubbing centers (15), Neustar is diluting its bandwidth capacity, making it less resilient to the largest DDoS attacks. If Prolexic had 15 scrubbing centers, it would have over 1 Tb of capacity.
Attack volume	Prolexic handles thousands of attacks each year – far more than any other provider. In addition, because of our client base and the "attack prone" industries they are in, we also fight the biggest and most complex attacks.	Neustar sees a fraction of the attack volume that Prolexic sees. That's critical, because in DDoS mitigation, experience is everything.
Layer 7 attacks	Prolexic has developed its own hardware, proprietary software, and processes to effectively mitigate Layer 7 attacks.	Ask Neustar how it detects and mitigates application layer (Layer 7) attacks. Ask how it handles a live hacker that changes tactics during a Layer 7 DDoS attack.
Randomized GET Flood DDoS Attack Mitigation Capabilities	Prolexic is the only provider able to mitigate and clean SSL post and GET FLOOD attacks.	Ask Neustar to demonstrate its pattern matching and "on the fly" signature creation capabilities.
Time to mitigate guarantee	Prolexic's time to mitigate is the fastest in the industry. In fact, Prolexic is the first company to integrate a 'Time to Mitigate' (TTM) SLA into its contract language (2010).	It is unlikely Neustar has the integrated event displays and coordinated network tools to match Prolexic's level of responsiveness to DDoS attacks. Ask Neustar for a SLA and read the fine print.
Mission critical client base	Prolexic's client base features global businesses with mission critical Internet facing infrastructures, including 5 of the world's 10 largest banks.	Verify Neustar's DDoS client list to be sure these companies are not UltraDNS customers instead. Be sure to obtain references from attacked customers and then compare.
Attack mitigation staff	Prolexic has a full-time staff that includes 40+ mitigation specialists and engineers. Our DDoS engineers spend 100% of their time focused on providing best-in-class mitigation services 24/7.	Ask Neustar which personnel in its organization spend 100% of their time fighting DDoS attacks.
PCI compliance	Prolexic is the first DDoS mitigation provider to secure PCI DSS (Payment Card Industry Data Security Standard) level 1 certification	Neustar is not PCI DSS certified for DDoS mitigation. If your industry requires certification, it will take time and cost money to audit Neustar.

1. "DDoS attack hobbles major sites, including Amazon", Tom Krazit, CNET, December 23, 2009

For More Information

To learn how Prolexic monitoring and mitigation services can protect your business from the largest, most sophisticated DDoS attacks, please visit **www.prolexic.com** or email **sales@prolexic.com**. You can also call us at **+1 (954) 620 6002**.

PROLEXIC
DDoS Attacks End Here.

v.02-29-12

DDoS Mitigation Services

Comparing Akamai and Prolexic

With so many providers offering Distributed Denial of Service (DDoS) mitigation, it can be confusing trying to determine which one is best for your needs. One important fact you should keep in mind is that while all vendors seem to claim the same thing – complete protection from DDoS attack – there is a significant difference in how these services are delivered and how successful they are.

Success with a multi-layered strategy

Prolexic is a pure play DDoS mitigation provider. It's all we do and all financial and human resources are devoted to DDoS monitoring and mitigation. In contrast, Akamai is a leading content delivery network that offers DDoS protection as an add-on service. While Prolexic and Akamai are competitors, we are also partners. We share hundreds of customers because our services are not just different, but also complementary. As such, if you are considering adding or indeed already have Akamai CDN or DDoS services, you should also consider adding Prolexic to the mix. After all, it has been proven that a multi-layered strategy can be very effective in reducing the impact of DDoS attacks.

To help in your decision and make it clear exactly what level of protection you are buying from Akamai and Prolexic, we've put together this helpful "cheat sheet". While it may seem there are a lot of small details to consider, it's the little things that make a big difference when your web site experiences a large, complex DDoS attack that can result in hours or even days offline.

Criteria	Prolexic	Akamai
Business focus	Prolexic has been 100% focused on DDoS mitigation since 2003. That's all we do.	Akamai's core business is providing web and content delivery services. DDoS mitigation is an add on service offering.
Mitigation vs. Absorption	Prolexic mitigates all DDoS attacks – whether high bandwidth, high pps (packets-per-second), encrypted or "low and slow" Layer 7 attacks that target web applications.	Akamai's Intelligent Platform is "designed to help customers absorb malicious traffic when under a DDoS attack."[1] This may work for some "old school" high bandwidth attacks, but it is of little use against today's more complex Layer 7 or multi-vector attacks.
Success rate	Prolexic has never failed to mitigate a DDoS attack – and we have handled the largest, most complex attacks ever launched.	Many global brands that use Akamai as a CDN have experienced protracted outages – sometimes as long as 72 hours – when also using Akamai's DDoS services and have had to engage Prolexic to mitigate the attack.
Infrastructure – network architecture	Prolexic's network is built around four scrubbing centers with extremely high bandwidth in each center. Centers are located in London, Hong Kong, Virginia and San Jose. Each scrubbing center is 100% dedicated to handling attack traffic. Prolexic's scrubbing centers are equipped in parallel – as redundant centers – with equipment capable of mitigating all types of DDoS attacks.	As a content delivery network, Akamai does not have an ideal network architecture for fighting DDoS attacks. While it can block simple Layer 3 and HTTP attacks directed to Akamai IPs, it does not protect against attacks targeting back-end IPs. To be an effective CDN, Akamai must allow legitimate looking requests and these can attack the customer's origin servers. An attacker who decides to flood the origin IP with a Layer 3 attack, spoof IP traffic from a subset of Akamai servers, or launches legitimate application requests, will bypass Akamai defenses completely. These techniques are widely known.

PROLEXIC
DDoS Attacks End Here.

Criteria	Prolexic	Akamai
Infrastructure – attack mitigation bandwidth	Prolexic operates the world's largest attack scrubbing network with Tier-1 global carriers. Prolexic has more than 375 Gbps of bandwidth and 100% of it is dedicated to DDoS attack traffic. No one comes close to matching this.	Akamai's network, while extremely large, is built to accelerate content delivery, not mitigate DDoS attacks. Akamai has thousands of smaller data centers that can be individually overwhelmed when facing a DDoS attack, causing short-term outages and latency increases as Akamai's DNS services identify and re-direct traffic. Attackers can target Akamai's IPs or spread attacks over more edge servers. If the botnet is not widely distributed it can overwhelm and degrade service for a large number of Akamai nodes.
Layer 7 attacks	Prolexic defends against all HTTP and HTTPS attacks, no matter how subtle. Prolexic is capable of analyzing ALL traffic in real-time and is able to rapidly identify targeted Layer 7 attacks. This is critical because a targeted Layer 7 attack composed of legitimate looking requests sent in at a reasonable rate can overload an application.	While Akamai has some firewall-like defenses for web applications, these have not scaled well to handle large HTTP and HTTPS attacks. Additionally, Akamai's DDoS Defender service places the responsibility of detection and mitigation of Layer 7 attacks onto the customer, effectively passing the Layer 7 attack through. Akamai is developing capchas and Javascript challenge technologies in their web servers, however these can affect SEO rankings, break AJAX and Restful technologies used in web applications, and more. While they may block some old-style botnets, increasingly sophisticated attackers can easily bypass these standard defenses. These approaches are also not compatible with NAT'ed and proxied traffic.
Monitoring	Prolexic offers both volumetric flow-based monitoring and Layer 7 application-based monitoring. Prolexic provides on-premise equipment to enable accurate, real-time monitoring and analysis of performance, applications and protocols.	Akamai does not monitor customer systems for DDoS attacks and only provides performance checks for http (not DNS or other protocols).
Back end IP protection	Prolexic goes beyond proxy offerings and can work with your data center and hosting or cloud providers at a more fundamental level to protect all inbound traffic in a subnet.	Akamai offers no back-end protection and instead shifts the burden to a customer's ISPs which either employ simple ACLs or extra-charge small-scale DDoS mitigation. Relying on ISPs is a bad idea as an ISP has no choice but to black-hole all traffic (i.e. render your site offline) if a DDoS gets too large. In addition, volumetric attacks against your real IP address space completely bypass Akamai's network.
Protection for other protocols including DNS	Prolexic protects a wide range of protocols. For example, Prolexic offers best-in class DNS protection and protects the world's largest registrars, DNS companies and root servers. Prolexic offers a protected DNS service and provides a separate hosted DNS service with tremendous capacity.	Akamai proxies HTTP and HTTPS and does not defend against DNS attacks. In addition, Akamai relies heavily on DNS to route traffic to its POPs. As a result, DNS attacks have caused significant and on-going disruption to Akamai's network and clients for several years.
Time to mitigate guarantee	Prolexic's time to mitigate is the fastest in the industry. In fact, Prolexic was the first company to integrate a "Time to Mitigate" (TTM) SLA into its contract language (2010). A Level 1 Prolexic technician based at our Security Operations Center can handle all customer attacks without escalation. This results in a rapid and focused response.	Akamai is a big company with many organizational layers. When you are under attack it may take many escalations to reach people who can help – and if your site is down and you rely on it for e-Commerce, even a few extra minutes can result in big losses.

About Prolexic

Prolexic is the world's largest, most trusted distributed denial of service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Fourteen of the world's twenty largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit **www.prolexic.com**, email **sales@prolexic.com** or call **+1 (954) 620 6002**.

1. http://www.eweek.com/c/a/Security/Akamai-Adds-AntiDDoS-Compliance-Management-to-Content-Delivery-Platform-206968/

v.02-29-12

PROLEXIC
DDoS Attacks End Here.

Tiny Sample Size Skews Results

Neustar Insights: DDoS Attack Trends 2010 - 2011

Attack Trends 2010-2011 makes for interesting reading. But before you think Neustar is an authoritative source on Distributed Denial of Service (DDoS) remember that they only began offering mitigation services in Q3 2011. Prolexic, on the other hand, is the world's largest, most trusted DDoS mitigation provider and we have been monitoring and mitigating attacks since 2003.

As we read through Neustar's report, we thought it was only right to point out some significant flaws.

Neustar on Q4 attack trends

> In 2010, more DDOS attacks occurred in Q4, during one of the busiest ecommerce seasons ever. In 2011, we saw the number of attacks decrease dramatically (-48.5%) in Q4 and throughout the year.

This is hard to believe and it's the polar opposite of Prolexic's data. Our data – gathered from a significantly larger sample of attacks – shows the number of attacks increasing by 2% in 2011 compared to 2010. What's more, Q4 is typically the busiest time for DDoS attacks due to e-Commerce providers being targeted in the run up to Christmas. Attackers typically time their attacks to create the most impact and havoc – and that means Q4. And here's the proof. Prolexic's data showed a 50% increase in the number of attacks from Q311 to Q411. It's hard to explain Neustar's plunge in Q4 attack numbers, other than the small sample size has skewed results.

Neustar on attack sizes

2010 Maximum Attack Size (Measured in Kpps)

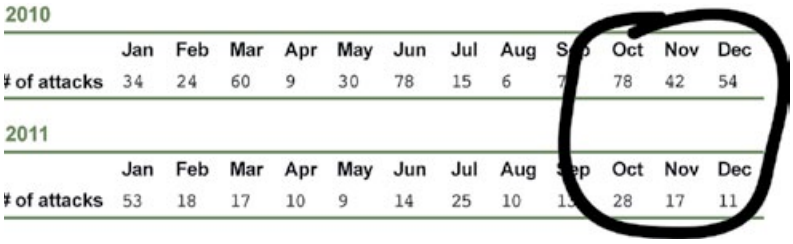
Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2	3	20	10	7	429	93	21	38	101	570	472

2011 Maximum Attack Size (Measured in Kpps)

Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
904	338	47	3,798	91	1,541	44	908	121	389	347	2,970

Compared to what Prolexic mitigates, these attack sizes are miniscule. For example, Neustar's largest mitigated attack (April 2011) was just 3,798 kpps or 3.8 Mpps. In contrast, Prolexic's largest 2011 mitigated per packet attack was 80 Mpps – over 20 times larger. Prolexic routinely sees – and mitigates effectively – the largest attacks launched in the world. That's why we invest heavily and have by far the world's largest attack mitigation network. Unlike other providers, this network is dedicated to mitigation – we don't piggy back other services onto it like Neustar does with DNS because that takes valuable bandwidth and can compromise effectiveness.

Neustar on number of attacks

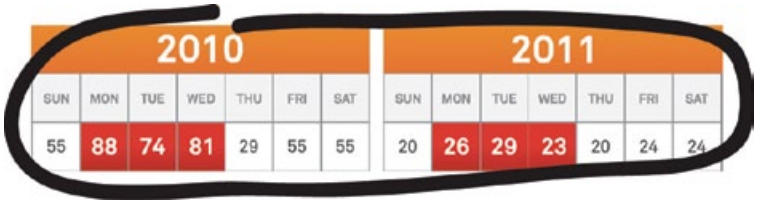


2010	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
# of attacks	34	24	60	9	30	78	15	6	7	78	42	54

2011	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
# of attacks	53	18	17	10	9	14	25	10	13	28	17	11

Neustar reports just 56 attacks for the entire Q4 period in 2011. Are they serious? Prolexic often mitigates more attacks than this in JUST ONE DAY. Because Neustar's attack sample is so small, it is very risky to draw any firm conclusions from this data. If Neustar had logged just 33 more attacks in Q4 – something Prolexic might see in a 12-hour period – then Q4 would have been the busiest quarter for attacks. See how easy it is to dramatically change conclusions when your sample set is so small?

Neustar on attack timing



2010	SUN	MON	TUE	WED	THU	FRI	SAT
	55	88	74	81	29	55	55

2011	SUN	MON	TUE	WED	THU	FRI	SAT
	20	26	29	23	20	24	24

When you're attacked it's disruptive no matter what day of the week it is. In contrast to Neustar's data, Prolexic sees more attacks on Saturdays than any other day. One interesting fact is that Saturday has been the top day for attacks two years running against Prolexic clients. Because of our significantly larger sample, we believe this is a more accurate depiction of reality. Saturdays would seem a logical day because many attackers probably work 9-5 in real jobs during the week.

Why you should trust Prolexic

Prolexic issues quarterly attack reports that give you up-to-date insight into what's really happening on the front lines. Data for each report has been gathered and analyzed by the Prolexic Security Engineering & Response Team (PLXsert). This group monitors malicious cyber threats globally and analyzes DDoS attacks using proprietary techniques and equipment. Through data forensics and post attack analysis, PLXsert is able to build a global view of DDoS attacks, which is shared with Prolexic customers. By identifying the sources and associated attributes of individual attacks, the PLXsert team helps organizations adopt best practices and make more informed, proactive decisions about DDoS threats. Because of our very large sample size, Prolexic's data and conclusions from it are likely to be more reliable.

Get the real facts

Want to really know what's going on in the world of DDoS? Go to **www.prolexic.com/attackreports** to download our latest report. Each attack report summarizes Prolexic's quarterly DDoS mitigation activities and provides valuable insight into the tactics, types, origins, and targets of these attacks.

For More Information

To learn how Prolexic monitoring and mitigation services can protect your business from the largest, most sophisticated DDoS attacks, please visit **www.prolexic.com**, email **sales@prolexic.com**, or call us at **+1 (954) 620 6002**.

PROLEXIC
DDoS Attacks End Here.

v.02-29-12

DDoS Mitigation Services

Comparing VeriSign & Prolexic

It's not easy being the industry leader. Competitors are constantly snapping at your heels, attempting to convince potential customers they are more cost effective or have better – or at least equal – capabilities. Despite what you are being told, no other provider measures up to Prolexic when it comes to Distributed Denial of Service (DDoS) monitoring and mitigation - not even VeriSign. But you don't have to take our word for it.

> *"VeriSign Inc, the company in charge of delivering people safely to more than half the world's websites, has been hacked repeatedly by outsiders who stole undisclosed information from the leading Internet infrastructure company."*
>
> **Joseph Menn, Reuters, 2/2/12**

In February 2012, Reuters reported that VeriSign – the company ultimately responsible for the integrity of Web addresses ending in .com, .net and .gov. – had been repeatedly hacked. While VeriSign executives "do not believe these attacks breached the servers that support our Domain Name System network," a breach of this nature could enable legitimate sites on the Internet to be imitated for nefarious purposes. If VeriSign cannot protect its own servers from hackers, do you really trust them to protect your critical web site from DDoS attacks?

To help you compare the facts about Prolexic and VeriSign, we've put together this "cheat sheet" so you know what level of service you are buying. Some of these points may seem minor now, but it's the little details that will make a huge impact on your business and web site availability when you are experiencing a DDoS attack.

PROLEXIC
DDoS Attacks End Here.

Criteria	Prolexic	VeriSign
Business focus	Prolexic has been 100% focused on DDoS mitigation since 2003. That's all we do and all we invest in.	VeriSign's core business is providing naming and authentication services. It offers DDoS monitoring and mitigation as an "add on" service and only recently made the service widely available (2010).[1]
Infrastructure – scrubbing centers	Prolexic currently has four global scrubbing centers located in London, Hong Kong, San Jose and Ashburn, VA. Each scrubbing center is 100% dedicated to handling attack traffic. Prolexic's scrubbing centers are equipped in parallel – as redundant centers – with equipment capable of mitigating all types of DDoS attacks.	VeriSign uses the same infrastructure to fight DDoS attacks and support DNS services, which is its core business. What happens when a large DDOS attack starts to overwhelm this network? It's likely that VeriSign will protect its core business and DNS customers – some of the largest networks on the Internet – by "blackholing" DDoS attack traffic which will take down your site. Is that what you signed up for?
Infrastructure – bandwidth	Prolexic has 500 Gbps of bandwidth and 100% of it is dedicated to DDoS attack traffic. No one comes close to matching this.	VeriSign has nowhere near the dedicated DDoS attack mitigating bandwidth that Prolexic has. Beware that transit capacity is not true attack mitigating capacity.
Infrastructure – network architecture	Prolexic's network is built around four scrubbing centers with extremely high bandwidth in each center. Balancing the attacks across scrubbing centers and having a scrubbing center close to the attack source is a proven strategy for success.	VeriSign's distributed "hub and spoke" model architecture increases latency and produces sub-optimal routing – and with more third parties involved there is a greater likelihood that traffic will be interrupted. This architecture can also create inconsistent any-casting of traffic.
Infrastructure – carriers	Prolexic selects carriers based on quality of service and capacity, not price. Prolexic uses the same three Tier-1 global carriers in all scrubbing centers identically so it can effectively manage high volume attacks by balancing traffic globally without manual intervention.	VeriSign does not use the same carriers globally, leading to suboptimal routing and outages caused by circuit saturation as it is not possible to cleanly and quickly balance and manage traffic for large DDoS attacks.
Attack volume	Prolexic handles thousands of attacks each year – far more than any other provider. In addition, because of our client base and the attack prone industries they are in, we also fight the biggest and most complex attacks. Prolexic regularly mitigates attacks over 50 Gbps.	Since VeriSign relies heavily on one vendor for mitigation (Arbor Networks), it is limited when it comes to fighting concurrent attacks as well as large attacks when they originate from one region (e.g. Asia), which could overload part of its network. Ask VeriSign to provide documentation of the largest attacks it has successfully mitigated and compare to Prolexic.
On premise equipment	Prolexic can provide on-premise mitigation equipment to speed traffic and attack analysis, leading to better, more informed decision making.	VeriSign does not offer on-premise equipment and while this reduces operational costs, it also sacrifices visibility into attack behavior.
Layer 7 attacks	Prolexic has developed its own hardware, proprietary software, and processes to effectively mitigate Layer 7 attacks.	Ask VeriSign how it detects and mitigates application layer (Layer 7) attacks. Ask how it handles a live hacker that changes tactics during a Layer 7 DDoS attack.
Randomized GET flood DDoS attack mitigation capabilities	Prolexic is the only provider able to mitigate and clean SSL post and GET flood attacks.	Ask VeriSign to demonstrate its pattern matching and "on the fly" signature creation capabilities.
Time to mitigate guarantee	Prolexic's time to mitigate is the fastest in the industry. In fact, Prolexic is the first company to integrate a 'Time to Mitigate' (TTM) SLA into its contract language (2010).	VeriSign only provides a time to react SLA - and reacting is not mitigating. Ask VeriSign for a time to mitigate SLA and read the fine print.
Responsiveness	When you call the Prolexic Security Operations Center, you'll get to speak with a technician who is mitigating your DDoS attack. That's a level of personalized customer service VeriSign cannot match.	VeriSign is a huge company and you'll be one of thousands of "accounts". The company's managed DNS service has over 6,400 customers for example[2]. It's more likely that the person who answers the phone will not be the one mitigating your attack – not what you want in an emergency situation.
Mission-critical client base	Prolexic's client base features global businesses with mission critical Internet facing infrastructures, including 6 of the world's 10 largest banks.	Ask VeriSign for a list of its DDoS clients and compare. See how many have mission-critical infrastructures in at-risk industries like e-Commerce and financial services.
Security Operations Center	Prolexic has a full-time staff dedicated to providing first-line mitigation services 24/7.	Ask Verisign how many of its personnel in its organization spend 100% of their time fighting DDoS attacks. It is likely some DDoS calls will have to be escalated to VeriSign's security team, which can add to delays and site downtime.

Criteria	Prolexic	VeriSign
Pricing Model	Prolexic does not charge a per attack fee so no matter how many times you are attacked during your contract period, the price remains the same. We keep it simple and you always know where you stand.	VeriSign charges a per attack fee, making accurate budgeting virtually impossible. And while pricing may appear low and attractive at the outset, it can escalate dramatically if you experience high attack volumes.
PCI compliance	Prolexic is the first DDoS mitigation provider to secure PCI DSS (Payment Card Industry Data Security Standard) level 1 certification.	VeriSign is not PCI DSS certified for DDoS mitigation. If your industry requires certification, it will take time and cost money to audit VeriSign.

It's a fact. Prolexic represents the gold standard for DDoS mitigation. While others claim to do what we do, when you look closely it's not even close. The simple truth is that in an industry of "me-too" providers making big promises, Prolexic stands alone as the world's first, largest and most trusted DDoS mitigation provider with unmatched experience, expertise and resources.

About Prolexic

Prolexic is the world's largest, most trusted distributed denial of service (DDoS) mitigation provider. Able to absorb the largest and most complex attacks ever launched, Prolexic restores mission critical Internet-facing infrastructures for global enterprises and government agencies within minutes. Fourteen of the world's twenty largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel/hospitality, gaming and other at-risk industries rely on Prolexic to protect their businesses. Founded in 2003 as the world's first "in the cloud" DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida and has scrubbing centers located in the Americas, Europe and Asia. For more information, visit **www.prolexic.com**, email **sales@prolexic.com**, or call us at **+1 (954) 620 6002**.

1. Source: http://www.networkworld.com/news/2011/050911-verisign-ddos.html
2. Source: http://www.computerworlduk.com/news/security/3278805/verisign-to-extend-cloud-based-ddos-protection-to-smes/

v.02-29-12

PROLEXIC
DDoS Attacks End Here.