Stop DDoS Attacks in Minutes

www.prolexic.com

PROLEXIC

DDoS Attacks End Here.

"The Prolexic DDoS mitigation package had a lot of things that the other companies just couldn't do."

Ryan McElrath, Chief Technology Officer, Americaneagle.com

You've seen the headlines. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are increasing in frequency, complexity and size. Because Internet-facing infrastructures are critical to revenue generation for most organizations, the impact of a DDoS attack can be catastrophic and widespread – affecting your ability to communicate, process transactions or function effectively for hours or even days.

Many organizations believe that it won't happen to them, but denial is no defense. On average there are more than 7,000 DoS and DDoS attacks observed daily – a number which is growing rapidly. And for those organizations that do expect the worst, the bad news is that the DDoS defenses they currently have in place – whether from an ISP, DNS provider, Content Delivery Network (CDN), telco or appliance – are unlikely to withstand the biggest multi-Gbps attacks. In an industry full of DDoS mitigation providers making big promises, only one company – Prolexic – has the expertise, experience and proven track record to detect and withstand the widest range of attack vectors with the fastest response time and lowest latency in the industry.

Mitigated the largest attacks in 2013:
167 Gbps and 144 Mpps

All resources focused
on DDoS mitigation
and network protection

Protects hundreds
of the world's
largest brands

The world's first (2003)
and largest (1.5 Tbps) cloud-
based mitigation platform

The gold standard in DDoS mitigation

It's a fact. Prolexic is the world's largest and most trusted DDoS mitigation provider. Founded in 2003, Prolexic was the first global, cloud-based DDoS mitigation service and our focus has never wavered: restoring the most complex, mission critical Internet facing infrastructures for global enterprises and government organizations.

Prolexic successfully mitigates tens of thousands of denial of service attack events each year, often mitigating the world's biggest attacks that overwhelm other providers. Of course, all providers loudly claim that they can handle any type and size of attack, but after hours of trying, many quietly pass their customers to Prolexic. The reality is that no other DDoS mitigation provider or DDoS attack is a match for Prolexic.

The fastest restoration in the industry

Prolexic does more than restore services after a DoS or DDoS attack. For the largest, most complex attacks, we do it faster than any other provider. Mitigation begins immediately and typical mitigation time is just 5-20 minutes after traffic starts flowing through Prolexic's scrubbing network. We were the first DDoS protection company to publish and stand behind a time to mitigate service level agreement (SLA) because for mission-critical applications, minutes count. For example, industry analyst firms estimate the cost of a 24-hour outage for a large e-Commerce company can approach US$30 million. Can you afford to take that risk with your business?

On-demand, cloud-based DDoS protection

Prolexic protects Internet facing infrastructures against all known types of DoS and DDoS attacks at the network, transport and application layers.

When an attack is detected, our protection services are implemented within minutes. Upon activation, a Prolexic customer routes in-bound traffic to the nearest global Prolexic scrubbing center where proprietary-filtering techniques, advanced routing, and patent-pending hardware devices remove bot traffic close to the source. Clean traffic is then routed back to the customer's network. Because we dedicate more bandwidth to attack traffic than any other provider – supplemented by proprietary tools, techniques, and experienced security experts – we have been able to handle the largest, most complex multi-vector DDoS attacks ever launched.
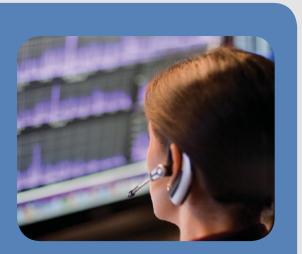
About DDoS attacks

A DDoS attack is an attempt to make a computer resource (i.e. website, e-mail, voice, or a whole network) unavailable to its intended users. By overwhelming it with data and/or requests, the target system either responds so slowly as to be unusable or crashes completely. The data volumes required to do this are typically achieved by a network of remotely controlled Zombie or botnet (robot network) computers. These have fallen under the control of an attacker, generally through the use of Trojan viruses. Prolexic currently tracks more than 4,000 command and control servers globally, which manipulate these botnets for attack, and we track more than 47 million bots in our global IP reputational database.

Some experts estimate that one quarter of Internet connected computers have been compromised and infected by one or multiple botnets. The scariest part of all is that in the cyber underworld, it is possible to rent 80,000 – 120,000 hosts capable of launching DDoS attacks of 10-100 Gbps – more than enough to take out practically any popular site on the Internet. The price? Just US$200 per 24 hours!

The Prolexic Portal — See what's happening on your network and ours

Continually enhanced and updated with new capabilities, the Prolexic Portal provides an up-to-the-minute view of what is happening on your network from a DDoS perspective, as well as what activities Prolexic is undertaking on your behalf. No other DDoS protection company provides this level of immediate insight and detail, making the portal an invaluable resource.

Click on graphs to zoom in and drill down into more detail for specific time frames. View reports. Create tickets. Access valuable resources. Use it daily as the command center of your proactive defense against DDoS threats.

In simple terms, defeating hackers is a game of cat and mouse. Because botnets and point and click DoS and DDoS attacks are becoming increasingly sophisticated, you'll need a provider that always keeps one step ahead. Unlike ISPs, DNS providers, CDNs and telcos, DDoS mitigation is our core business, not an add on service. Because DoS and DDoS protection is our singular focus, we devote all human and financial resources to developing proprietary monitoring and mitigation tools and techniques that you won't find anywhere else in the industry.

But that's not all. Prolexic has the largest DDoS mitigation staff of any provider, 10 years of real-world experience, and has built its solution from the best mitigation equipment available – all tested in our lab under real-world attack conditions. This is augmented, expanded and strengthened with proprietary technologies, routing and techniques to address zero-day attacks.

In addition, Prolexic operates a 24/7/365 Security Operations Center (SOC) staffed by a team of front-line DDoS protection experts. This is critical because many attacks are concerted efforts by live attackers and the characteristics of the attack can change during the attack itself. Success against the most sophisticated hackers can only be achieved by reacting in real time and supplementing automated tools with human expertise. In this way, it is possible to distribute attack loads and combat attacks with characteristics that have never been seen before. This is just not possible with the use of off-the-shelf technology alone.

Of course, building and maintaining this level of expertise is not easy. That's why each Prolexic SOC engineer spends 20 percent of their time in advanced training sessions. They meet to discuss, develop and learn about new techniques, strategies and tools that can be applied on behalf of our clients.

Getting to grips with Layer 7 attacks

Complex Layer 7 attacks often resemble legitimate traffic and requests, making them hard to detect. Unlike more common regular bandwidth floods, Layer 7 attacks can be structured to overload specific elements of an application server infrastructure. Even simple attacks – for example those targeting login pages with random user IDs and passwords, or repetitive random searches on dynamic websites – can critically overload CPUs and databases. Prolexic has developed leading edge proprietary tools that consistently detect and mitigate Layer 7 attacks with an unmatched level of success.

Prolexic's broad portfolio of field-proven solutions can keep your business protected against today's large and complex denial of service attacks, including the increasingly common high bandwidth attacks that many providers struggle to mitigate.

MONITORING

OPTIONS

PLXfbm

PLXsert

PLXabm

PLXproxy

PLXrouted

PLXconnect

MITIGATION

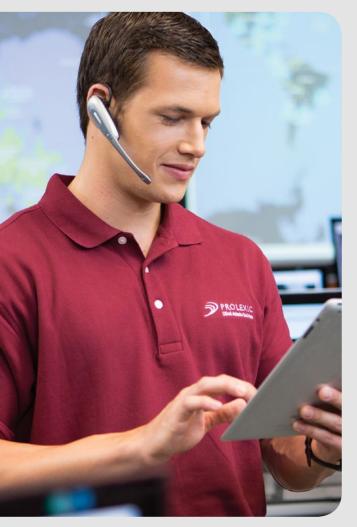| Attack Category	TTM - Time to Mitigate Typical	TTM - Time to Mitigate Guaranteed (SLA)
UDP/ICMP Floods	1 minute or less	5 minutes
SYN Floods	1 minute or less	5 minutes
TCP Flag Abuses	1 minute or less	5 minutes
GET/POST Floods	10 minutes or less	20 minutes
DNS Reflection	5 minutes or less	10 minutes
DNS Attack	5 minutes or less	10 minutes

Prolexic monitoring services

- **PLXfbm (Flow-based monitoring)** – Provides early detection and notification of DDoS attacks by monitoring customer routers directly. With Prolexic's attack monitoring service, you can rely on Prolexic's 24/7 SOC to detect anomalies, perform impact analyses, and notify your personnel of conditions that could threaten your networks. The information will provide a clear recommended action plan, which may include switching to immediate protection by re-routing traffic through the Prolexic Protection Network. This service may be combined with PLXabm which alerts on Layer 7 (application layer) abuses to HTTP and HTTPS traffic.

- **PLXabm (Application-based monitoring)** – An easy-to-deploy, remotely managed solution that provides real-time monitoring and detection of application layer attacks. This on-premise solution puts Prolexic's botnet detection expertise on your network for precise traffic and attack analysis. Our proven HTTP anomaly detection and traffic analysis tools automatically profile HTTP traffic and provide the capability to detect HTTP GET, POST and other abuses (including low/slow permutation attacks) and address SSL/SSH encrypted-layer cyber attacks.

Prolexic mitigation services

- **PLXrouted (Activation via route advertisement)** – The preferred method of activation for enterprise-class businesses, this service provides protection for all services, ports and protocols while providing total control over when traffic is filtered. DoS and DDoS attacks are detected by monitoring customer premise equipment and the service is activated using Border Gateway Protocol (BGP) to onramp traffic to Prolexic's cloud-based mitigation infrastructure.
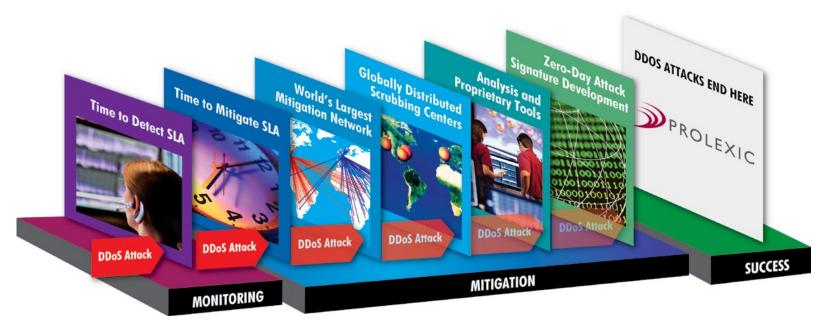
- **PLXconnect (Activation via route advertisement)** – This service delivers Prolexic's routed DDoS protection service over a direct physical connection from your network through a private MPLS network to our scrubbing centers. PLXconnect is ideal for organizations with large networks and complex application interactions that need predictable latency and high throughput.

- **PLXproxy (Activation via DNS redirect)** – This service allows a Prolexic customer to initiate a DNS change to redirect all network traffic through Prolexic where it is cleansed. Suitable for small to medium businesses and all firms under immediate attack, this is the quickest way to provision Prolexic's DDoS mitigation protection.

Optional services

- **PLXsert (Prolexic Security Engineering & Response Team)** – A subscription service that provides pre- and post-attack insight and intelligence on DDoS attacks. PLXsert monitors malicious cyber threats globally and analyzes attacks using proprietary techniques and equipment. 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 DoS and DDoS threats. A PLXsert subscription includes post-attack forensics, exclusive Emergency Threat Advisories, and access to Prolexic's IP Reputational Database Feed, which provides details on active botnets.

"Through 2016, the financial impact of cybercrime will grow 10 percent per year, due to the continuing discovery of new vulnerabilities."

"Gartner's Top Predictions for IT Organizations and Users, 2012 and Beyond: Control Slips Away," (www.gartner.com)

Discourage attacks with Prolexic

Prolexic not only mitigates attacks once they start, but actually discourages attackers from launching attacks in the first place. Prolexic's reputation and our unrivaled mitigation capabilities are very well known throughout the world and it's easy to find out that network traffic will be or is being routed through Prolexic. Any experienced attacker knows it's a waste of their time and bandwidth trying to bring your services down when the world's largest attack mitigation network stands in the way.

Contact our Protected by Prolexic team at **protected@prolexic.com** for more information on program incentives and how to get started.

"We like the way that Prolexic can stop attacks immediately when we route the traffic through their servers."

Denise Vella, Information Security Officer, Entropay

Prolexic gives you more

- **More capacity**: No one has a larger, global mitigation network to absorb the biggest DDoS denial of service attacks. No one.

- **More responsiveness**: Prolexic begins DDoS attack mitigation within minutes – and we have a service level agreement (SLA) to prove it.

- **More experience**: Prolexic fights more DDoS denial of service attacks than many of our competitors combined – tens of thousands of DDoS attacks each year – and we've been doing it successfully longer than anyone else.

- **More expertise**: Prolexic classifies and identifies more than 100 different types of DDoS attacks and offers DDoS protection services capable of mitigating ALL of them – even new variants that have only just emerged.

- **More support**: Our security operations center monitors DDoS attacks 24/7/365, compiles intelligence on thousands of botnets, and informs you immediately when we detect a DDoS attack that could affect your network.

- **More flexibility**: We offer a range of service levels and options to meet the needs of any business.

- **More peace of mind**: No attacker has been too smart and no denial of service attack has been too big or complex for Prolexic's protection.

Understand your risk. Become prepared. Ensure availability.

Malicious hackers are adept at uncovering hidden vulnerabilities in your Internet-facing infrastructure – but are you? PLXplanner is a suite of tools that helps you pinpoint gaps and risks in your DDoS protection strategy, so you can take proactive steps to stay ahead of malicious hackers – and keep your network and websites running 24x7. PLXplanner generates a custom report based on your unique IT and networking environment, helping you prepare your best possible DDoS defense. To get started, visit **www.prolexic.com/plxplanner**.

"Prolexic gives us the strong insurance policy against DDoS attacks that we were looking for."

Mark Johnson, Chief Financial Officer, RealVision

PLXpatrol

Get an instant global snapshot of current DDoS threats and activity

Staying informed about DoS and DDoS threats is the best defense against cyber attacks. Prolexic makes it easy with PLXpatrol, a free service available at **www.prolexic.com/plxpatrol**.

PLXpatrol includes:

- **Attack Tracker** — Continuously updated, this view shows where DDoS attacks directed against Prolexic's clients are originating from and the geographic location of attack targets.

- **Country Ranking** (Last 24 hours) — This ranking shows the countries that have originated the most attack traffic against Prolexic clients over the last 24 hours.

- **Country Ranking** (All Time) — This ranking shows the countries that have originated the most attack traffic against Prolexic clients since data collection began in 2009.

Prolexic will be adding new views in 2013 and beyond to give you even more in-depth insight into DoS, DDoS, and other emerging cyber threats. The information presented in PLXpatrol is sourced from Prolexic's analytical and IP reputational databases. Prolexic makes this information, and more detailed views, available to its customers in near real-time through the Prolexic Portal.

> Stop DDoS attacks in minutes

Turn the tables. Protect your business. Ensure continuity even under the largest attacks. To do all that you only need one company: Prolexic. For more information on how Prolexic can protect your organization from spiraling DDoS attacks, please contact **+1 (954) 620 6002** or **sales@prolexic.com**.

About Prolexic:

Prolexic Technologies is the world's largest, most trusted distributed denial of service (DDoS) protection and mitigation service provider. Able to absorb the largest and most complex DDoS attacks ever launched, Prolexic protects and restores within minutes mission-critical Internet-facing infrastructures for global enterprises and government agencies. Ten of the world's largest banks and the leading companies in e-Commerce, SaaS, payment processing, travel, hospitality, gaming and other industries at risk for DDoS attacks rely on Prolexic for DDoS protection. Founded in 2003 as the world's first in-the-cloud DDoS mitigation platform, Prolexic is headquartered in Hollywood, Florida, and has DDoS scrubbing centers located in the Americas, Europe and Asia. To learn more about how Prolexic can stop DDoS attacks and protect your business, please visit www.prolexic.com, call +1 (954) 620 6002 or follow @Prolexic on Twitter.

PROLEXIC
DDoS Attacks End Here.