

# Stop DDoS Attacks in Minutes



[www.prolexic.com](http://www.prolexic.com)

 **PROLEXIC**  
DDoS Attacks End Here.

**PREVENTIA**

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

Mark Johnson, Chief Financial Officer, RealVision

You've seen the headlines. Distributed Denial of Service (DDoS) attacks are increasing in frequency, complexity, bandwidth and size. Because Internet-facing infrastructures are critical to the profitability of 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 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 mitigation providers making big promises, only one company – Prolexic – has the expertise, experience and proven track record to detect and withstand all attacks. That's why DDoS attacks end here.



### > About DDoS attacks

A DDoS attack is an attempt to make a computer resource (i.e. web site, 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 10 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 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.

We do more than successfully mitigate tens of thousands of attack events each year. We mitigate 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 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?

*"Yola looked for a best-in-class partner that could maintain service uptime and mitigate all types of DDoS attacks, no matter how large or complex. After reviewing many options, Yola selected Prolexic."*

Lisa Retief, Vice President of Engineering, Yola

## On-demand, cloud-based mitigation

Prolexic protects Internet facing infrastructures against all known types of DDoS attacks at the network, transport and application layers. We do this through our distributed global network of scrubbing centers.

When an attack is detected, our protection services are implemented within minutes. Upon activation, a Prolexic customer routes in-bound traffic to the nearest 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.

In simple terms, defeating hackers is a game of cat and mouse. Because botnets and "point and click" 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 DDoS mitigation 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, nine years of real world experience, and has built its solution from the best mitigation equipment available – all tested in our lab under simulated attack conditions. This is augmented 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 experts. This is critical because many attacks are concerted efforts by "live" attackers and as a result, 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 when you have to wait days or even weeks for a software patch.



### > Getting to grips with Layer 7 attacks

Lately, more and more hackers have been adding complex Layer 7 attacks that resemble legitimate traffic to their DDoS attempts. Layer 7 attacks accounted for 26.5% of attacks against Prolexic clients in 2011. 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 web sites – 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.



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

Of course, building and maintaining this level of expertise is not easy. That's why 20% of Prolexic's fixed costs are allocated to training – that's one full day a week of training for each SOC expert. They meet to discuss, develop and learn about new techniques, strategies and tools that can be applied on behalf of our clients.

### > Prolexic gives you more

- **More capacity:** 500 Gbps of globally-distributed bandwidth available specifically for DDoS traffic.
- **More responsiveness:** Prolexic begins mitigation within minutes – and we have an SLA to prove it.
- **More experience:** Prolexic fights more DDoS attacks than many of our competitors combined – tens of thousands each year.
- **More support:** Our Security Operations Center monitors attacks 24/7/365, informs you immediately, and shares intelligence on botnets.
- **More flexibility:** Choose the level of service and options that are right for your organization.
- **More peace of mind:** No attacker has been too smart and no DDoS attack has been too big or complex for Prolexic.

"We had already begun to research who the leaders in DDoS mitigation were and, after talking to many engineers, Prolexic was the name that kept coming up."

Sohrab Jahanbani, Chief Operating Officer, GoNabit

"DDoS services are nearing 'must-have' status."

"Hype Cycle for Infrastructure Protection, 2011," Gartner, 8/10/11

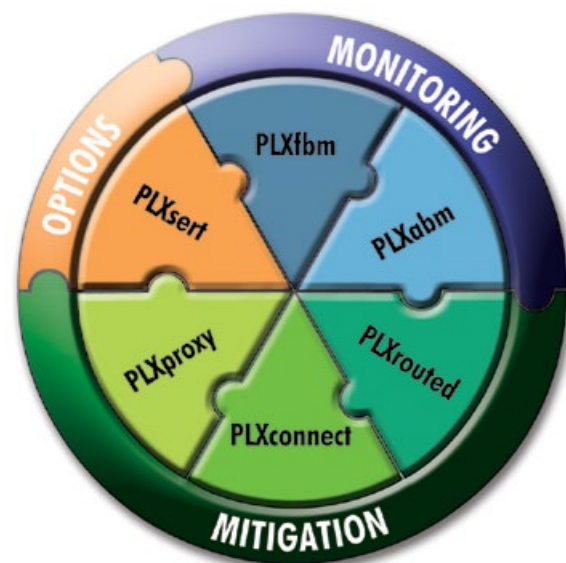
Prolexic's broad portfolio of field-proven solutions can keep your business protected against today's large and complex attacks, including the increasingly common high bandwidth attacks that many providers struggle to mitigate.

### 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 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 Floods (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. 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 mitigation service over a direct physical connection from your network through a private Prolexic cloud 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)** – A Prolexic customer initiates 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)** – 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 customers. Each quarter, PLXsert publishes an attack report summarizing Prolexic's mitigation activities and attacks against its clients. A free copy can be downloaded from [www.prolexic.com/attackreports](http://www.prolexic.com/attackreports).

- **IP reputational database** – Prolexic aggregates intelligence information from multiple sources and publishes the Prolexic IP Reputational database to partners detailing active botnets and fraud linked IP addresses.

### > 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.



## > 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](mailto:sales@prolexic.com).

### 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. Ten of the world's 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](http://www.prolexic.com).