

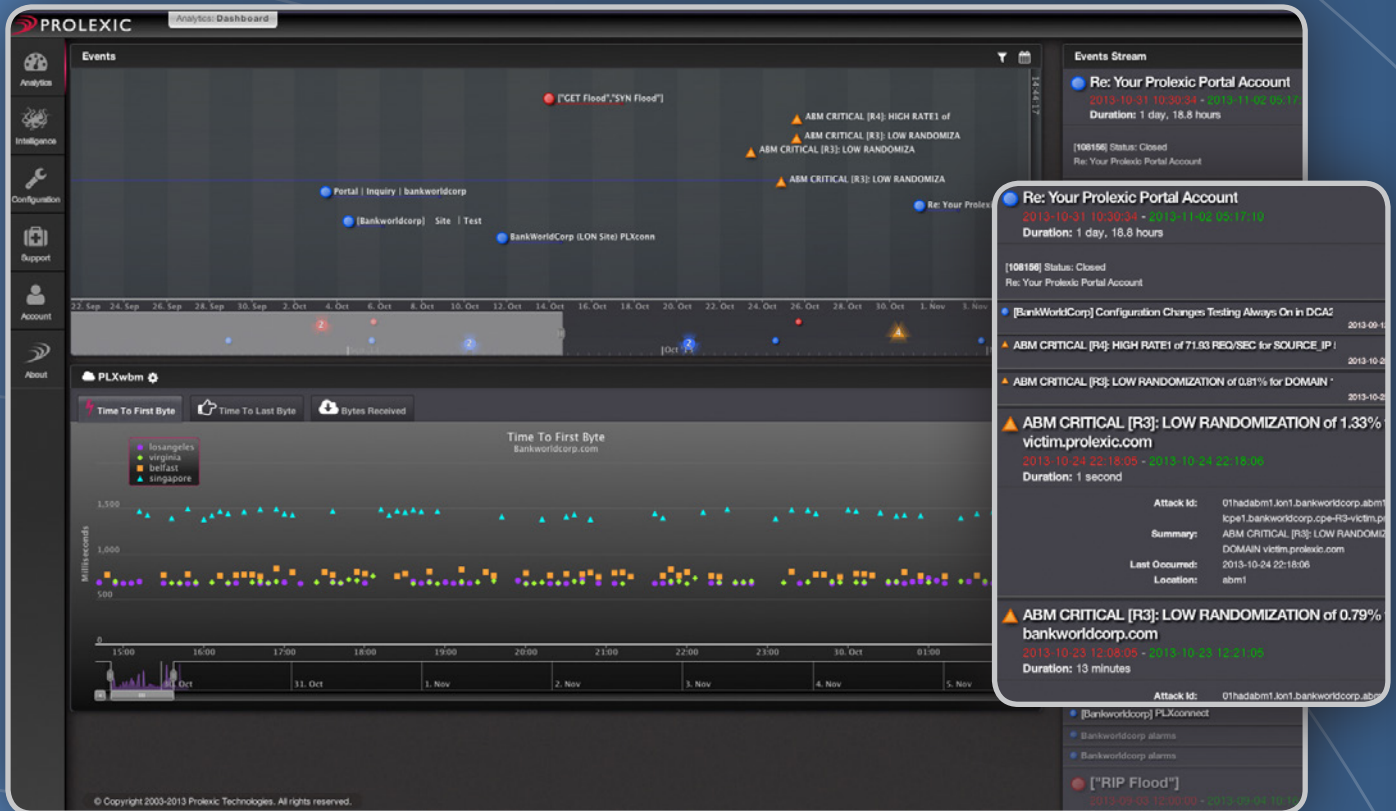


PLXportal

Deeper network visibility Real-time analytics Rich DDoS forensics

www.prolexic.com

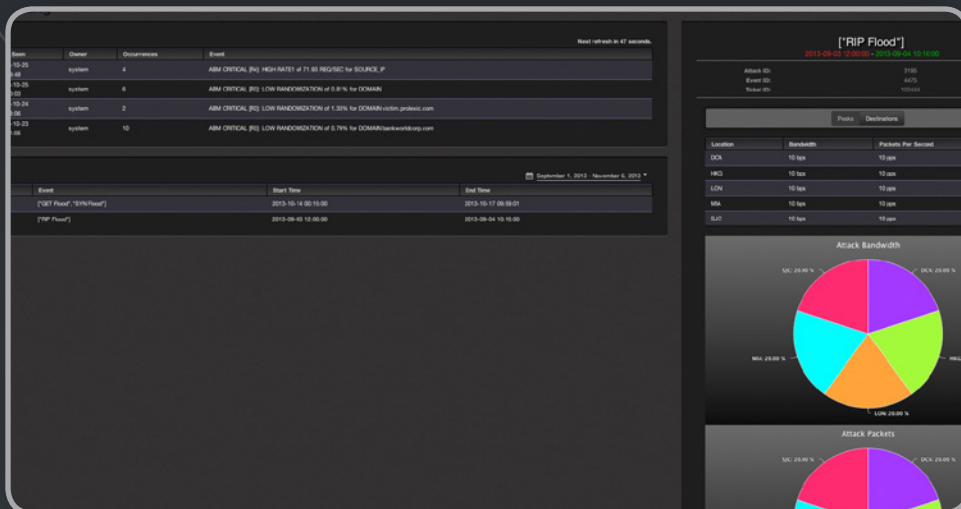
PROLEXIC
DDoS Attacks End Here.



Open the door to real-time visibility

Your network is under a Distributed Denial of Service (DDoS) attack. What do you do first? How big is the attack? What's the attack vector and how is the attack affecting specific elements in your network? If you were a Prolexic customer, you would be able to answer these questions instantly by logging in to the enhanced PLXportal – now with deeper real-time network views, more attack analytics, and optimized for tablets and other mobile devices.

PLXportal is a secure online resource that gives Prolexic customers a real-time view of what is happening on their network and the Prolexic mitigation infrastructure before, during, and after a DDoS attack or other network-affecting event. Prolexic customers can also access real-time intelligence and alerts provided by the Prolexic Security Engineering and Response Team (PLXsert), access a robust set of account management tools, and use a secure wizard to upload SSL encryption keys to Prolexic. Now you can manage all of your Prolexic services conveniently from a single screen.



See the big picture of network activity in one dashboard

PLXportal helps bring order to the chaos during a DDoS attack. We give our customers access to real-time network data that was previously only seen by our Security Operations Center (SOC) mitigation engineers. With more than one-third of Prolexic's customers currently running on the Prolexic network at all times for DDoS protection, we have enhanced the PLXportal user experience with deeper visualization of data and event timing analytics that are meaningful to any customer who routes onto Prolexic.

Only Prolexic Byte customers get the most granular DDoS threat data in real-time, including:

- Views of real-time HTTP and HTTPS request patterns for live traffic
- Views of attack traffic distribution and attack behavior
- Attack reports and SOC alerts
- Views of the latest DDoS threat intelligence compiled by PLXsert

The industry's best view of DDoS threats

Seconds count when defending against DDoS attacks. That's why Prolexic continually updates PLXportal with additional views and more granular DDoS threat data. For example, traffic information is updated in real-time. As such, Prolexic is able to deliver the industry's fastest mitigation while providing the information you need to make better, faster, more informed decisions.



The screenshot displays the PROLEXIC PLXproxy Analytics dashboard. It features a sidebar with navigation options: Analytics, Intelligence, Configuration, Support, Account, and About. The main content area is titled 'PLXproxy Analytics' and includes sub-tabs for 'HTTP Analytics' and 'Request Analytics'. The dashboard contains three tables under the heading 'Request Analytics':

Source IP Address		Requested Domains		Requested URLs	
IP Address	Count	Domain	Count	URL	
1.107.191.217	266265	portal.prolexic.com	1359878	portal.prolexic.com/dashboard/getProducts	
1.92.129.41	157648	www.prolexic.com	1341301	portal.prolexic.com/login	
1.151.109.17	124712	fbm.prolexic.com	252662	fbm.prolexic.com/page?id=mssp_customer_	
1.9.132.155	117186	legacyportal.prolexic...	80251	portal.prolexic.com/dashboard/getgraphdata	
1.107.191.217	116286	prolexic.com	37515	portal.prolexic.com/	
1.92.129.41	101850	unknown.prolexic.com	24432	www.prolexic.com/	
1.107.191.217	87530	portal.prolexic.com	10833	portal.prolexic.com/dashboard	
1.92.129.41	85828	www.prolexic.com	7538	portal.prolexic.com/dashboard/gettimegider	
1.151.109.17	82995	fbm.prolexic.com	6816	www.prolexic.com/assets/imgs/banner.png	
1.9.132.155	77830	legacyportal.prolexic...	2550	portal.prolexic.com/assets/font/fontawesom	
1.107.191.217	69396	prolexic.com	2239	portal.prolexic.com/themes/default/js/vende	



Introducing PLXwbm – Web-based monitoring

PLXwbm is Prolexic's proprietary site performance monitoring tool that's integrated within the Prolexic Cloud Security Platform:

- Quickly detect and respond to site performance issues
- Troubleshoot latency on your network and view performance over time
- Track performance during incidents to determine the effect of any network events
- Ensure website availability through faster issue detection and analysis
- Easily configure and change monitoring preferences in PLXportal

Only Prolexic customers can use PLXportal to quickly see the big picture of network activity and anomalies that may indicate DDoS attacks or other anomalous activity that affects your network's edge. Armed with this comprehensive view of network traffic and access to a rich store of alerts from multiple monitoring points, Prolexic customers can be proactive against DDoS threats.

See more with PLXportal



PLXportal is another giant leap forward in its evolution as a robust single-pane view of the broadest range of alert types from multiple monitoring points, real-time network views, and global cyber threat intelligence. As a result, you can benefit from:

Enhanced PLXportal dashboard

- Watch your traffic as it traverses Prolexic's network in a single view
- Customize views of traffic information, metrics, alerts, tickets, and events in a comprehensive view with an intuitive interactive time glider
- Filter information to the desired level of detail to best understand the composition and timing of traffic

Optimized views for mobile devices

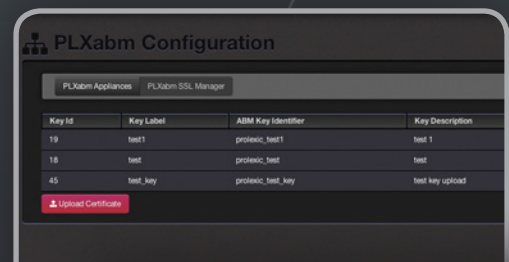
- You can access PLXportal from anywhere there is Internet access – on a tablet, phone or on any computer

New intelligence

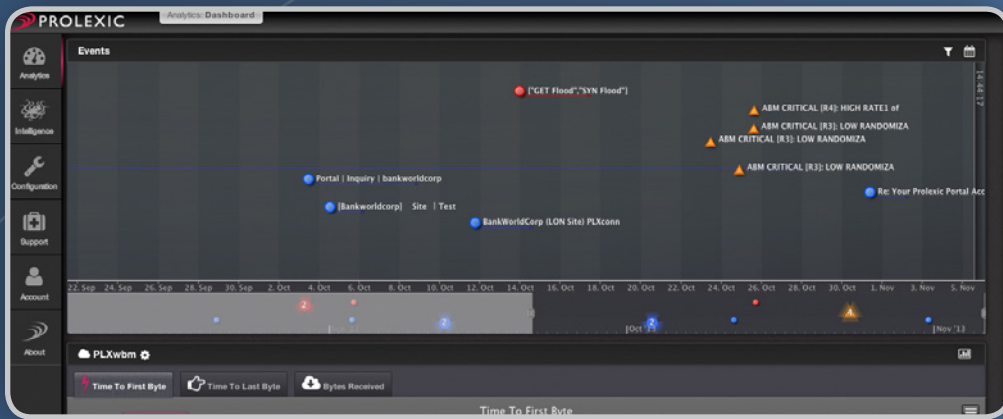
- Access the latest DDoS threat information compiled by PLXsert
- View attack traffic distribution and attacker behavior globally from PLXpatrol, which is updated throughout the day, every day

New PLXabm analytics view

- Upload and deploy certificates and keys securely using the new SSL Manager
- Gain a more detailed view of PLXabm application based monitoring with a new mapping display, advance filtering, and advanced searching

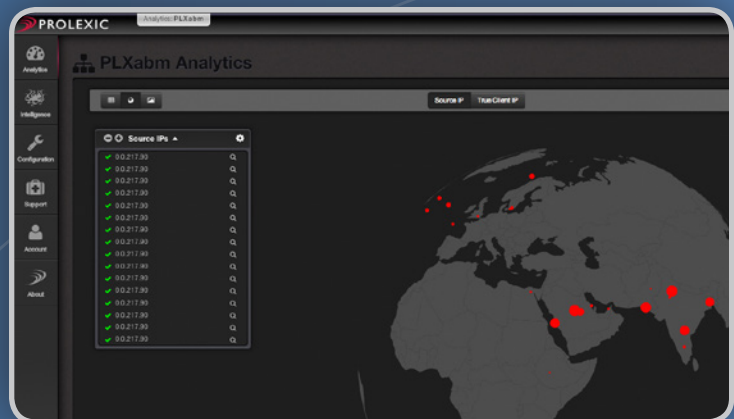


How to use PLXportal



Scenario: Always-on subscriber. DDoS attack detected and mitigated.

- **Monitor** - Visually review present traffic levels against recent and historical norms. Drill down to volume data by end point, protocol and Prolexic scrubbing center.
- **Detect** - Traffic is already being monitored by Prolexic for malicious activity. Alerts of network anomalies appear on the PLXportal dashboard.
- **Notify** - Prolexic will create a ticket upon detection and immediately begin to mitigate. Clients can also easily create a ticket via PLXportal or by calling the 24x7 SOC team.
- **Mitigate** - View Prolexic's mitigation efforts on your behalf and the impact on network traffic.
- **Analyze** - PLXabm subscribers and customers actively routed on the Prolexic network can view the primary source of Layer 7 traffic across 30 different attributes.
- **Communicate** - Submit tickets to Prolexic's SOC directly from the PLXportal dashboard.
- **Evaluate** - View alerts, attack logs, and other details of the attack, as well as a timeline correlation of events for a better understanding of detection, mitigation, and network events.



Scenario: Post-DDoS attack timeline analysis

After an attack has subsided, Prolexic customers can run forensics and view the individual events as they occurred to understand the scale of the DDoS attack and the impact on the network. You can also review your team's communication with Prolexic staff during the attack. By request, Prolexic can also provide post-attack forensics to law enforcement agencies and that data can be viewed anytime in the PLXportal.

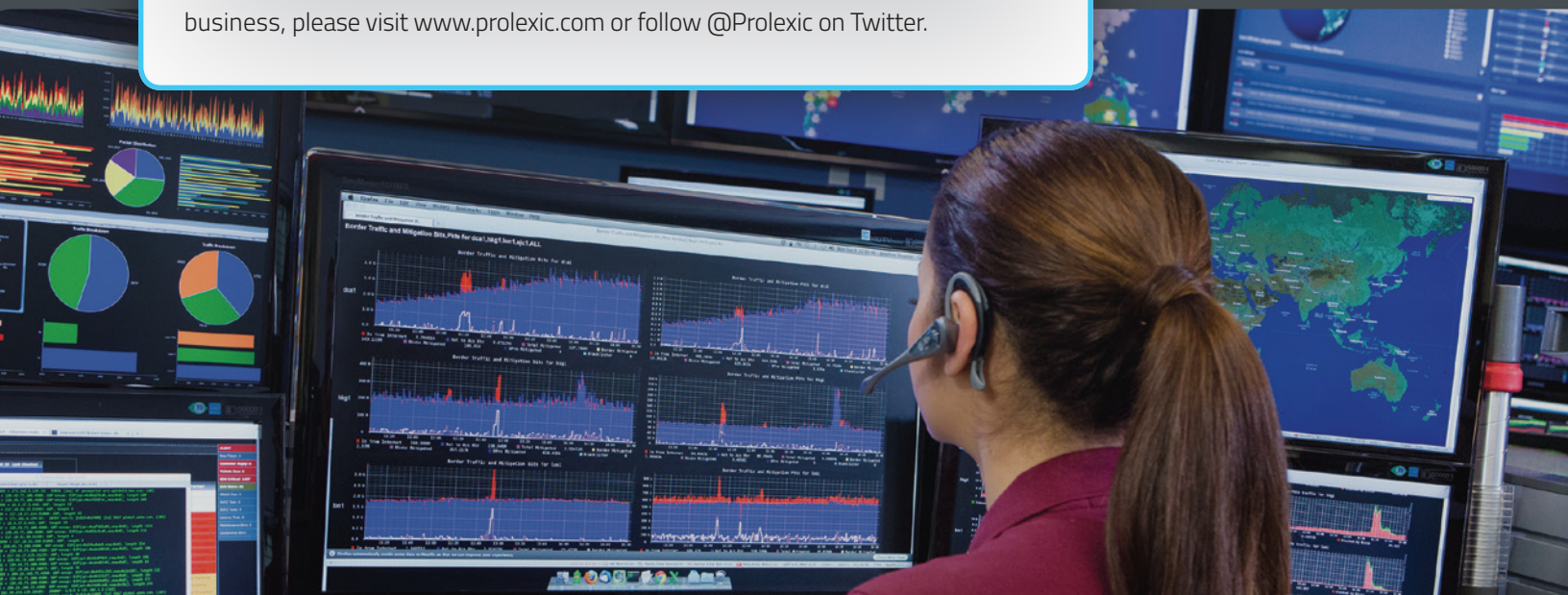
Prolexic customers can use the attack analytics as a roadmap to improve their preparedness for future DDoS incidents. For example, if attack analytics show that your network is vulnerable to GET floods, you might decide to address rate limiting problems. After any DDoS attack, PLXportal enables customers to mine rich data to help analyze the DNA of the attack – all in a single dashboard.

Become a Prolexic customer

Only Prolexic customers have access to PLXportal – but if you aren't yet a Prolexic customer, we want to show you what you've been missing. Visit www.prolexic.com/plxportal to watch the PLXportal video. You can also visit www.prolexic.com/plxpatrol to view a small sample of the DDoS intelligence Prolexic provides through PLXportal. Then contact us at +1 (888) 368 2923 or +001 (954) 620 6005, or insidesales@prolexic.com to discuss the many other advantages of being a Prolexic customer.

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, energy, 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 or follow @Prolexic on Twitter.





The Prolexic Cloud Security Platform





The DDoS and cyber threat landscape is changing – for the worse. Over the past year alone, a dramatic shift to server-based attack platforms has led to some of the largest attack sizes ever recorded – gigabits per second rates that are nearly three times larger than last year. Cyber adversaries such as Al Qassam and Anonymous have become bolder and more sophisticated as evidenced by a resurgence of DNS attack vectors and a devastating series of attacks on the financial services sector.

Prolexic is changing cyber security – for the better. Our Cloud Security Platform goes far beyond Distributed Denial of Service (DDoS) mitigation. Experience the next generation of cyber security – one that provides more capacity, more analytics and more threat visibility than ever before.

Introducing the Prolexic Cloud Security Platform


The Prolexic Cloud Security Platform is the next generation of Prolexic's security infrastructure – built to be the largest and strongest DDoS mitigation network in the world to ensure the availability of our customers' networks. Enhanced with greater capacity and redundancy, our geographically distributed Cloud Security Platform supports the delivery of Prolexic's gold standard DDoS mitigation services, plus holistic views of network monitoring and the delivery of rich real-time analytics with options for "on-demand", "always-on", or hybrid service models. Choose from connectivity options via proxy, GRE tunnel or direct connection via MPLS backbone for the greatest flexibility in fortifying your network against DDoS and other cyber threats.

The network architecture of the Prolexic Cloud Security Platform takes cyber security to a higher level by:

- Deploying 1.8 Tbps of attack bandwidth in our data centers by Q4 2013 – and upgrading that capacity to 3 Tbps over the next year
- Doubling capacity in our existing data centers and adding new state-of-the-art data centers in Frankfurt, Sydney, and Tokyo, designed solely for DDoS and cyber-attack mitigation
- Scaling out attack mitigation, analytics capabilities, and attack countermeasures horizontally to support faster DDoS attack detection and mitigation
- Capturing billions of data points for expanded cyber threat detection and correlation
- Gathering and measuring analytics separate from mitigation without increasing latency for more robust inspection and blocking methodologies



Most of all, as DDoS and other types of cyber threats evolve and change over time, the defenses within the Prolexic Cloud Security Platform will evolve with them to provide the best and fastest resolution for all of the possible cyber-attacks that can touch our customers.



The Prolexic Cloud Security Platform is proof of our commitment to providing the highest level of both DDoS mitigation services and the full realm of cyber security services. We have changed our network architecture to accommodate organizations that want always-on DDoS protection and an added level of cyber security to further reduce the risks to their network and business overall.

Increased threat visibility. Reduced risk.

Prolexic first solves the DDoS issue — ensuring the availability of our customers' websites. Then we apply our vast expertise in DDoS to other cyber threats. Instead of juggling multiple providers and portals, Prolexic can provide more rapid and detailed attack detection, immediate mitigation, and a unified view of cyber threats because your traffic is already flowing through our network. With access to the Prolexic Cloud Security Platform – an extensible network with planned future services – you receive so many advantages:

- 24/7 network monitoring
- Flow-based monitoring capabilities (Layer 3 and 4 attacks)
- Application-based monitoring capabilities (Layer 7 attacks)
- More accurate alerting for a wider range of threats
- Faster and more detailed cyber-attack detection and root cause analysis
- Immediate assessment and rapid DDoS mitigation following a critical alert
- No 24/7 staff required to redirect traffic when using PLXedge
- Real-time network analytics visible in PLXportal 24x7
- The same access to actionable analytics that our SOC technicians have
- Automatic updates – no reconfiguration needed

Building a more diverse cyber threat defense

Prolexic is more than just a leading DDoS mitigation service provider. When you route your network traffic through the Prolexic Cloud Security Platform – either when under a DDoS attack or continuously as an always-on PLXedge customer – you can take a stronger and more confident defense against cyber-attacks with our gold-standard DDoS monitoring and mitigation expertise, deep network analytics, and expanded web monitoring. But what sets the Prolexic Cloud Security Platform apart is a robust, resilient cloud-based infrastructure that supports a broader platform of cyber security services beyond DDoS – so Prolexic customers will be ready to defend against any and all cyber threats now and years from now.

Prolexic is a premier cyber security provider – not just an insurance policy against DDoS.

PLXedge for premier DDoS protection

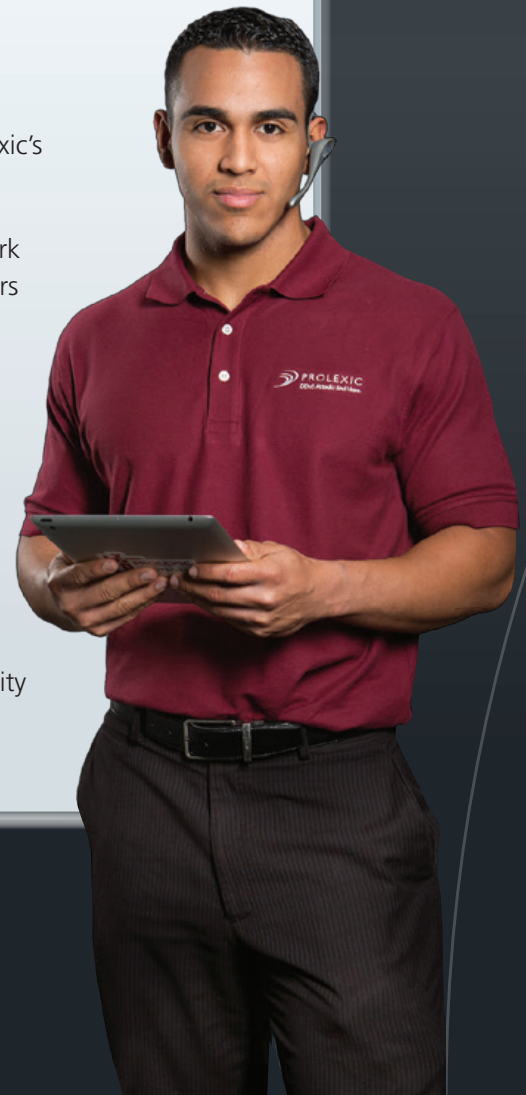
Defeat DDoS and other cyber threats with the world's largest and most hardened network specifically designed for mitigating cyber-attacks. Delivered through the Prolexic Cloud Security Platform, PLXedge is Prolexic's premier bundled solution of mitigation, monitoring, and analytics services that can stop the largest DDoS attacks on the Internet.

PLXedge delivers comprehensive, always on protection through our industry-leading DDoS mitigation expertise, DDoS alerting for both Layer 3 and 4 volumetric attacks and Layer 7 application attacks, real-time network analytics, and Web-based monitoring (PLXwbm). All PLXedge alerts, network views, attack forensics, and reports are immediately accessible through the secure PLXportal – available only to Prolexic customers.

Why PLXedge?

- Get the strongest cloud-based, always-on DDoS protection with Prolexic's industry leading time-to-mitigate SLA
- Ensure the minimum downtime with the richest real-time 24/7 network monitoring and rapid mitigation by the best DDoS mitigation engineers in the industry
- Faster and more granular cyber-attack detection at IOS layers 3, 4, and 7 and root cause analysis of even the largest DDoS attacks on the Internet
- Minimum impact on latency and user experience

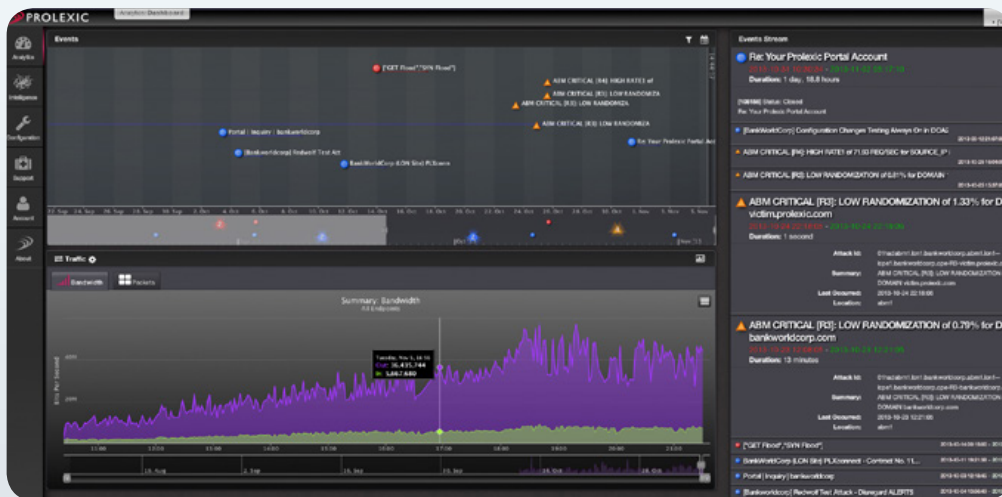
Through PLXedge, Prolexic will be able to analyze and store analytic data across key dimensions to identify malicious behavior. PLXedge customers will benefit from customized alerting and messaging when malicious activity is detected – delivering a broader scope of protection from cyber threats.



Real-time visibility in PLXportal

See everything you need in a single dashboard to manage your specific Prolexic Cloud Security Platform services. PLXportal is a secure online resource that gives Prolexic customers a real-time view of what is happening on their network and the Prolexic Cloud Security Platform before, during, and after a denial of service attack. Prolexic customers can also access real-time DDoS intelligence and alerts provided by the Prolexic Security Engineering and Response Team (PLXsert) and use a robust set of account management tools.

Prolexic continually refreshes PLXportal views and provides the industry's most granular DDoS threat data. In addition, DDoS attack forensics are updated every 1 to 5 minutes - significantly faster than any other mitigation provider. And now you can take PLXportal with you. PLXportal can be viewed anywhere there is Internet access via Smartphone, iPhone, touch screen device, or any PC browsers.



Stay protected on the Prolexic Cloud Security Platform

The Internet continues to be a very dangerous place. That's why Prolexic continues to invest heavily in restructuring our proven DDoS mitigation infrastructure with expanded capacity, stronger tactical response capabilities, and enhanced redundancy to defend our customers against the largest and most sophisticated cyber-attacks observed today – and five years from now. Stay protected with Prolexic against DDoS and strengthen your tactical response capabilities against the growing menace of cyber threats.

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, energy, 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 6005 or follow @Prolexic on Twitter.



PLXedge

Prolexic's Premier DDoS Mitigation, Monitoring, and Analytics Service



What

- PLXedge, Prolexic's premier DDoS mitigation, monitoring, and analytics services bundled on the world's largest cyber security network

How

- 1.8 Tbps of dedicated mitigation bandwidth – and growing
- 24/7 monitoring and mitigation by Prolexic DDoS mitigation experts
- Immediate inspection of traffic upon alert, and rapid mitigation deployment as required
- Rich, real-time analytics
- Rapid detection and root cause analysis
- Blacklisting for IPs during mitigation
- Immediate Layer 7 signature creation and deployment by our top DDoS experts
- Packet analysis at line rate and granular monitoring tools at layers 3, 4, and 7
- Web based Monitoring included for website availability monitoring and metrics

Why

- 24/7 protection against all types and sizes of DDoS attack vectors
- PLXedge ensures minimum downtime
- Protection backed by Prolexic's unrivaled time-to-mitigate SLA
- Minimum impact on latency and the user experience
- Gain greater network visibility through PLXportal

Delivered through the Prolexic Cloud Security Platform, PLXedge is Prolexic's premier cloud security and DDoS mitigation, monitoring, and analytics solution designed to rapidly detect and stop the largest DDoS attacks on the Internet. PLXedge includes everything you need for complete protection and peace-of-mind:

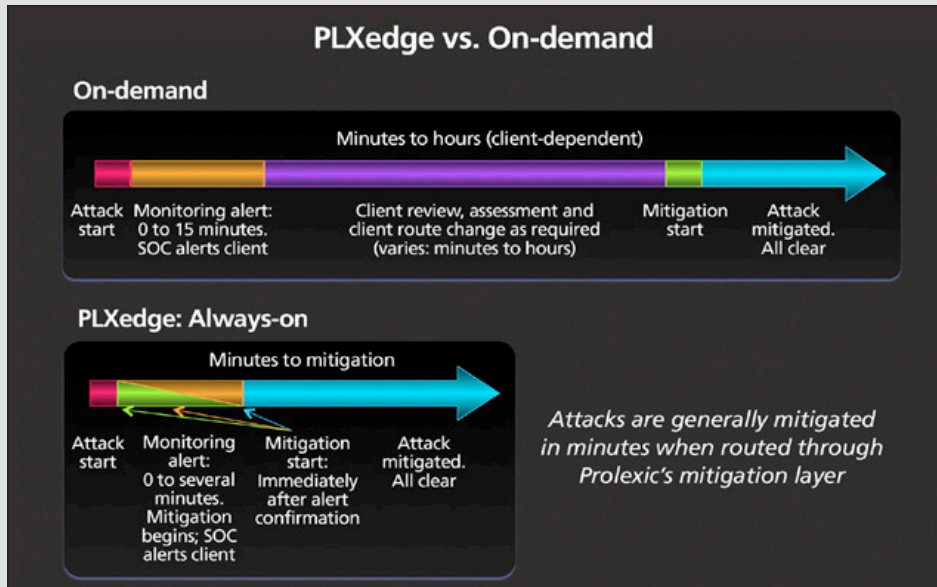
- 24/7 monitoring of customer traffic
- Industry-leading DDoS mitigation
- DDoS monitoring & alerting for Layer 3 & 4 volumetric attacks
- DDoS monitoring & alerting for Layer 7 application attacks
- Near real-time network analytics
- Web-based monitoring (PLXwbm)
- Analysis of global botnet activity and proactive threat alerts based upon sophisticated correlation of events across industries, regions, IPs, and other patterns
- Plus, all PLXedge alerts, network views, attack forensics, and reports are immediately accessible through the secure PLXportal

Stay protected 24/7 against all DDoS attack vectors and emerging cyber threats. No other DDoS mitigation service provider can give you the breadth and depth of real-time intelligence, live mitigation expertise, and dedicated cyber security experience that you'll get with PLXedge.

How PLXedge works

PLXedge delivers high-level always-on DDoS protection through our industry-leading DDoS mitigation and monitoring expertise, which includes Layers 3 and 4 volumetric attack monitoring, Layer 7 http and https application monitoring, real-time network analytics, external web-based monitoring (PLXwbm) and complete mitigation coverage.

Because your network traffic is always flowing through PLXedge, it's only minutes to detection and mitigation. When the Prolexic Security Operations Center (SOC) team detects a DDoS attack, it immediately sends you a monitoring alert. Prolexic begins mitigation immediately following a critical alert, inspection, and confirmation of DDoS traffic.



Here's why PLXedge is the world's premier protection against DDoS and cyber threats:

- The best perimeter monitoring and alerting, covering all types of DDoS attack vectors and the largest attacks on the Internet
- Attacks mitigated in minutes – faster than any other DDoS mitigation service
- More visibility – all PLXedge alerts, network views, attack forensics, and reports are immediately accessible through the secure PLXportal – available only to Prolexic customers
- The richest, largest volume and dimensions of real-time information to support faster mitigation
- No in-house staffing required and no need to “route on” to Prolexic

Through PLXedge, Prolexic also collects and stores analytics across key dimensions to identify malicious behavior using new algorithms across multiple customers. We use this information to quickly develop customized alerting and messaging when malicious activity is detected – delivering a broader scope of defense against multiple types of cyber threats through PLXedge.

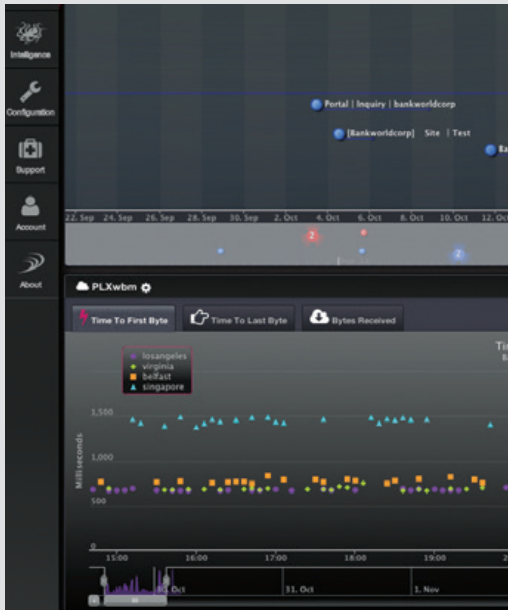
Stay protected 24/7 against cyber threats

When it comes to DDoS protection, don't settle for less than the world's largest dedicated cyber security network. As a service of the Prolexic Cloud Security Platform, PLXedge gives you the highest level of always-on DDoS mitigation protection and the rich analytics you need to ramp up your DDoS defense strategy. Call us and learn how Prolexic can protect your network today.

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, energy, 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 6005 or follow @Prolexic on Twitter.

Prolexic Web-Based Monitoring (PLXwbm)

Better, faster, easier website performance monitoring



What

- PLXwbm, Prolexic's proprietary site performance monitoring tool that runs on the Prolexic Cloud Security Platform

How

- Strategically placed web request initiating nodes
- Nodes report the status of URLs into a central aggregator for display
- View a recent history of latency from a global perspective in PLXportal

Why

- React faster to resolve website performance issues
- Diagnose performance problems more accurately
- Troubleshoot network latency and view performance over time
- Add another layer of DDoS detection to ensure website availability

What would it cost your organization if your website was down for 10 minutes, or if 10 percent of your customers couldn't access your online services? What if it was due to a DDoS attack? And what if you didn't know it?

Prolexic lets you know if your website is performing as expected, or not. Web Based Monitoring (PLXwbm) is an integrated component of the Prolexic Cloud Security Platform. PLXwbm is available whenever a customer's traffic is routing through the Prolexic Cloud Security Platform, whether through our "always-on" PLXedge service or as part of our on-demand PLXrouted or PLXproxy mitigation services. All Prolexic customers get free use of PLXwbm to monitor one URL through the secure PLXportal and monitoring for additional URLs can be purchased.

Prolexic has set up web-based monitoring sensors around the world to help our customers more quickly detect and respond to site performance issues. Why PLXwbm? Because Prolexic knows that a high performing website is critical for retaining customers, ensuring a strong revenue stream, and even maintaining a better search engine ranking. Most of all, our PLXwbm service is another way of monitoring your website for early detection of DDoS attacks – and preventing financial loss and other adverse effects of site downtime.

Integrate WBM with DDoS protection

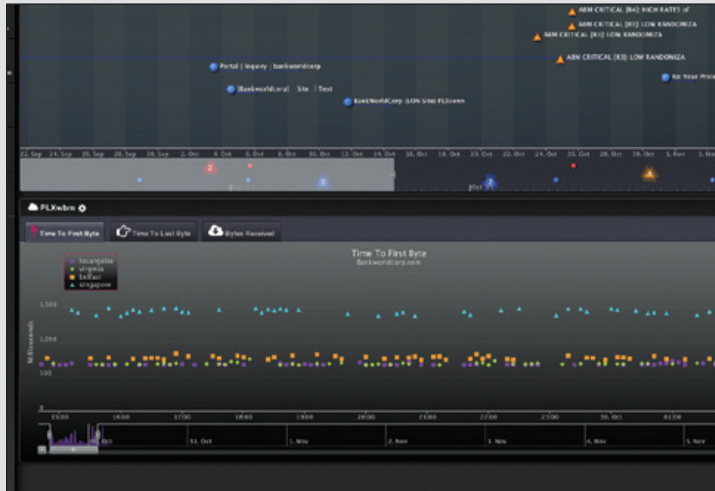
Now you can make website performance monitoring a strategic part of your DDoS protection arsenal – without having to purchase an additional third-party tool. Delivered through the Prolexic Cloud Security Platform, PLXwbm is available 24/7 within PLXedge, Prolexic's always-on bundled solution that includes our industry-leading DDoS mitigation, DDoS alerting for both Layers 3 and 4 volumetric attacks and Layer 7 application behavior attacks for HTTP, as well as network analytics. In addition to PLXwbm site performance analytics, all PLXedge alerts, network views, attack forensics, and reports are immediately accessible to Prolexic customers through the secure PLXportal.

Prolexic Web-Based Monitoring (PLXwbm)

How PLXwbm works

Prolexic developed PLXwbm so you can monitor global website uptime and performance – either through our PLXedge always-on DDoS mitigation service or when our on-demand services are activated.

PLXwbm is powered by a collection of strategically placed polling nodes and testing nodes, which report the status of your URL every few minutes. This site performance data flows into a central aggregator where it is available for display through PLXportal.



The secure PLXportal makes it easy for all Prolexic customers to view a recent history of site latency from a global perspective in a central monitoring window – all with a single login to the Portal and access to the intuitive Portal dashboard. View historic latency graphs, activity from distributed polling network sites, time to first byte, time to last byte, and detailed response results to support fast and accurate troubleshooting before, during, and after a DDoS attack.

The PLXwbm view through PLXportal also lets customers:

- View the global experience when attempting to load their website
- View latency performance over time as experienced from global polling locations
- Ensure website availability through faster reaction to problems and rapid resolution

Viewing PLXwbm data through the PLXportal also eliminates the complexity of using a third-party web-based monitoring service because you can easily view network and website performance analytics – plus DDoS attack alerts and forensics and Prolexic’s mitigation activity on your behalf – in one integrated system.

Protect against DDoS with Prolexic. Ensure website availability with PLXwbm

What you can't see can hurt you when it comes to website performance issues that could be caused by a distributed denial of service attack. Prolexic helps you ensure your website's availability – and protection against all DDoS threats – in the Prolexic Cloud Security Platform. Contact us to learn more about the advantages of a DDoS defense strategy with integrated web based monitoring through PLXwbm.

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, energy, 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 6005 or follow @Prolexic on Twitter.



DDoS Monitoring: Application Based (PLXabm)

Layer 7 DDoS attack monitoring and analysis

PLXabm (application-based monitoring) is a complementary monitoring service to PLXfbm (flow based monitoring) that focuses on the application layer. You can now leverage on-site the proprietary technology and analytic expertise that Prolexic uses in its Security Operations Center. By tracking 25 unique dimensions, PLXabm makes it possible to monitor and identify sophisticated Layer 7 abuses, service attacks and fraudulent activities that cause the greatest financial impact to online businesses.

The benefits of a managed Layer 7 monitoring service

With PLXabm, Prolexic technicians can take the data generated by an on-premise appliance and gain immediate insight into the “conversation” taking place between the client and server at the application level. Consequently, they can identify and analyze malicious Layer 7 traffic – and its variants in randomized attacks – easier and faster than ever before. This provides the ability to send early warning alerts to customers for more proactive DDoS protection and more informed decision making.

PLXabm helps Prolexic technicians analyze Layer 7 traffic faster and in more depth by performing these advanced monitoring capabilities:

- Passive analysis that is safe as there is no additional hardware in the traffic flow
- Data fed from network tap or switch SPAN port
- Ability to decode all standard HTTP headers including the true-client IP header used by most CDNs
- Privacy-aware correlation model protects customer data
- Fast alerting: instantaneous correlation on sensor can generate alerts in 15 seconds
- Powerful historical correlation across multiple sensors using historical data and IP reputation
- Correlation model detailed down to URLs and individual transactions, including over 20 HTTP headers
- Analysis performed on-premise with mitigation performed in Prolexic’s scrubbing cloud
- CDN / proxy / load balancer aware
- Identifies many attack types that intrusion protection systems, Web firewalls and load balancers miss

WHAT

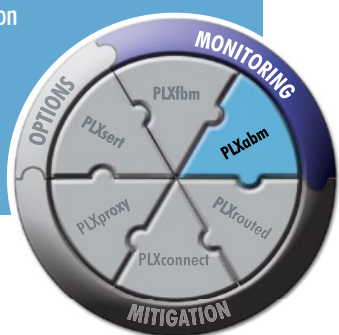
- A subscription service that leverages an on-premise appliance to provide 24/7 visibility into Layer 7 DDoS attacks
- The industry’s most detailed real-time analytical engine

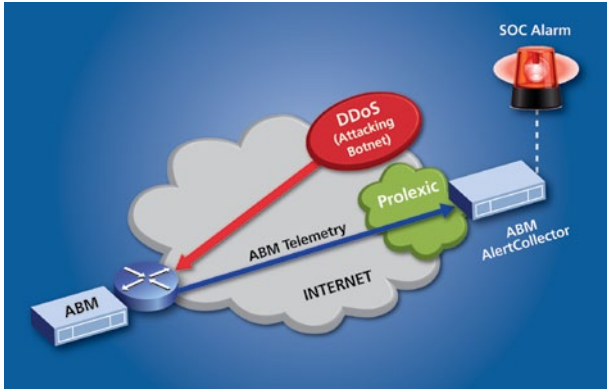
HOW

- Correlates millions of data points per second across 25 dimensions
- High performance engine decodes up to 40,000 HTTP requests per second
- Enables real-time forensic analysis at the application level

WHY

- Brings the analytical intelligence of Prolexic’s Security Operations Center (SOC) to your network 24/7 to assist in analysis and root cause identification
- Enables deeper and faster analysis of more attack types (“low and slow” Layer 7, randomized HTTP and more) that can’t be detected by load balancers and intrusion detection systems
- Provides the foundation for proactive analysis and mitigation to minimize downtime





How PLXabm works

Prolexic's on-premise PLXabm appliance collects and sends data back to Prolexic's Security Operations Center (SOC) where alerts, long-term statistical metrics, baselines, and forensic sets are created.

Armed with this information, Prolexic's SOC helps customers by pinpointing the precise nature of an attack in minutes. Once the distributed denial of service attack vector and attacker behavior are identified, the PLXabm appliance is configured to automatically send attacker information back to Prolexic to mitigate in the cloud. The feedback loop between local appliance and cloud mitigation is unique in the industry. The PLXabm service provides instant-on expertise to identify and analyze DDoS attacks as well as the strongest cloud defense to mitigate attacks.

Secure encryption key handling with PLXabm SSL

Prolexic also offers PLXabm SSL, which uses FIPS-140-2 Level 2 Hardware Security Modules (HSMs) deployed within a Prolexic PLXabm appliance at a customer site. Built on proven proprietary Prolexic technology used in our scrubbing centers, the PLXabm SSL decrypts SSL traffic enabling our DDoS mitigation engineers to identify and isolate the source IPs passively. The bots generating encrypted Layer 7 attacks can then be blocked in the cloud without Prolexic handling or looking at your SSL keys.

DDoS attacks detected by PLXabm

Attack Type	Detection
TCP abuse	No
UDP flood	No
ICMP flood	No
GET/POST flood	Yes

Fight Layer 7 attacks smarter, faster with Prolexic PLXabm

Prolexic's Application Based Monitoring service gives you the ultimate defense against malicious hackers and their Layer 7 attacks as it helps you fight back smarter and faster. Contact us at **+1 (954) 620 6002** or **sales@prolexic.com** to learn how Prolexic can better protect your business with PLXabm.

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.

DDoS Monitoring: Flow Based (PLXfbm)

Layer 3 and 4 distributed denial of service (DDoS) attack monitoring and analysis

Flow-based DDoS attack monitoring provides early detection and notification of DDoS attacks by directly monitoring customer edge routers. With Prolexic's flow-based attack monitoring service (PLXfbm), you can rely on Prolexic's 24/7 Security Operations Center (SOC) to detect anomalies, perform impact analyses, and notify your personnel of conditions that could threaten your networks. The information provided by Prolexic's SOC 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 Prolexic's Application Based Monitoring Service (PLXabm), which alerts on Layer 7 (application layer) abuses to HTTP and HTTPS traffic.

WHAT

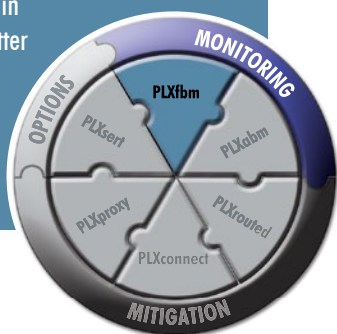
- A subscription service that provides 24/7 alerting on Layer 3 and Layer 4 DDoS attacks
- A solid foundation for DDoS monitoring at the network edge

HOW

- 24/7 remote monitoring by Prolexic's Security Operations Center (SOC)
- No additional on-site equipment to install
- Industry's fastest notification of possible attack traffic by phone or e-mail

WHY

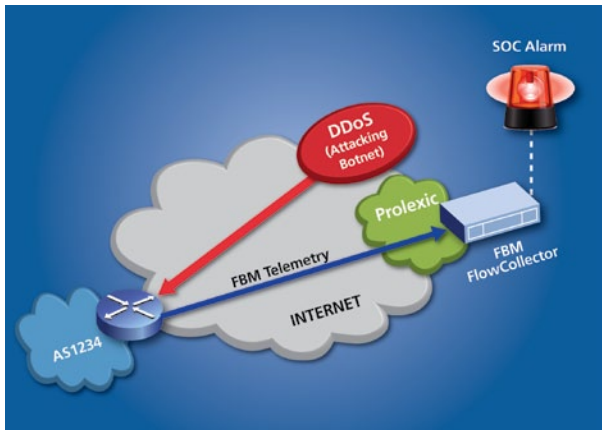
- Brings the analytical intelligence of Prolexic's SOC to your network for more informed decision making and peace of mind
- Provides a solid foundation for DDoS monitoring, resulting in proactive mitigation that minimizes downtime
- Avoids classic errors in configuration for better and more accurate performance monitoring



What makes PLXfbm DDoS detection service different

You can't fight and defeat malicious traffic if you can't identify it as such – and you don't want to risk blocking legitimate users from your site. PLXfbm service detects changes in volumetric traffic flows during Layer 3 and 4 DDoS attacks by monitoring profile changes on Internet edge routers. But that's where the similarity to other FBM services ends. Prolexic offers true remote flow-based monitoring with the added value of:

- **Singular focus** – Prolexic's SOC is not distracted by the need to monitor or oversee non-DDoS related business lines.
- **Proven DDoS expertise** – Prolexic mitigates more DDoS attacks than anyone else – 10 to 80 per day – and we have logged over 30,000 successful mitigations to prove our expertise in identifying and defeating all types of network attacks.
- **24/7 experience and the industry's fastest response** – PLXfbm customers are protected by the world's most experienced DDoS technicians in our 24/7 SOC. Prolexic technicians use the most advanced flow based monitoring tools to detect, analyze, and mitigate Layer 3 and 4 DDoS attacks faster than any other service provider. And we have the SLA to back it up.
- **Unmatched alert accuracy** – We provide an optimal configuration template for PLXfbm customers to avoid classic errors in balancing the performance and accuracy of the PLXfbm system and the resource demands placed on edge routers. The result is fewer false positives and greater peace of mind that Layer 3 and 4 DDoS attacks will be detected quickly and accurately.



The benefits of a managed Layer 3 and 4 DDoS monitoring service

With the PLXfbm DDoS detection service you will gain the confidence that your online presence is protected 24/7 from distributed denial of service attacks that can make your site perform slowly or become completely inaccessible – and cause your business to lose millions of dollars per hour of downtime. In addition, Prolexic’s approach to FBM using advanced DDoS monitoring tools delivers benefits that include:

- **Non-Intrusive** – Does not insert additional hardware in the traffic flow, minimizing any potential impact to services.
- **Continuous expert DDoS monitoring** – Prolexic SOC technicians immediately detect anomalies in your network traffic, analyze them, and determine whether or not to have you on-ramp your traffic.

How PLXfbm DDoS detection works

Prolexic technicians in the SOC go through a process of fine tuning the PLXfbm system to determine a

profile of your traffic patterns. That profile is then continually updated so that our technicians are constantly learning what your traffic looks like at any given time. Drawing upon that knowledge, they can instantly recognize significant deviations from the baseline, begin immediate analysis, and alert you if there is a DDoS attack in 15 minutes or less.

DDoS attacks detected by PLXfbm

Attack Type	Detection
TCP abuse	Yes*
UDP flood	Yes
ICMP flood	Yes
GET/POST flood	No
HTTPS flood	No

*Provided TCP flag data is included in router Netflow

DDoS detection is further enhanced by subscribing to Prolexic’s Application Based Monitoring Service.

Be ready to fight DDoS attacks faster with PLXfbm

Distributed denial of service attacks are now a mainstream threat and the number of DDoS attacks continues to escalate – no business or organization is safe from being the target of malicious cyber criminals. Make Prolexic’s Flow Based Monitoring service your first line of defense against Layer 3 and 4 DDoS attacks and empower your business to fight back faster and smarter. Contact us at **+1 (954) 620 6002** or **sales@prolexic.com** to learn how Prolexic can better protect your business with PLXfbm.

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.

DDoS Mitigation: PLXconnect

High bandwidth connectivity for on-demand DoS and DDoS mitigation

The PLXconnect Service Plan delivers Prolexic's routed DoS and DDoS denial of service mitigation service over a direct physical connection from your network through a private Prolexic cloud to our scrubbing centers.

Like Generic Route Encapsulation (GRE), this physical connection enables you to easily activate Prolexic DDoS protection for an entire subnet, enabling redirection of Internet traffic to the Prolexic network during a distributed denial of service attack and away from the Prolexic network during non-attack periods. Unlike GRE, there is no impact to Maximum Transmission Units (MTUs), latency is predictable, and you can achieve much higher throughput. Best of all, PLXconnect has the highest performance SLA in the industry to extend the peace of mind you always have with Prolexic.

Why Prolexic PLXconnect

You should choose PLXconnect if you:

- Desire a higher bandwidth connection to Prolexic
- Want to eliminate the overhead of GRE tunnels
- Operate a complex Internet edge deployment using many protocols and site-to-site VPNs
- Use applications that do not accommodate lower maximum packet size

How Prolexic PLXconnect works

Prolexic's PLXconnect Routed Service Plan relies on a physical connection to a private cloud to allow Prolexic to onramp the customer's incoming traffic and inspect it for anomalies or misbehaviors. We identify all legitimate traffic and forward it on its normal path, while silently dropping attack traffic.

The BGP routing protocol is used to communicate network advertisements from your site to Prolexic. You use these network advertisements to activate and deactivate the service as needed. Activation is complete when Prolexic communicates these advertisements to its upstream carriers and peers from each of its scrubbing facilities, a process that normally occurs in a few seconds. Traffic is then cleansed and forwarded to the customer's router(s). Over the course of this interception process, outgoing traffic from your servers to the Internet is always forwarded as normal to your ISP(s). This approach, called asymmetric routing, maximizes the benefits of Prolexic's scrubbing process while minimizing the overall impact on your typical traffic flow.

WHAT

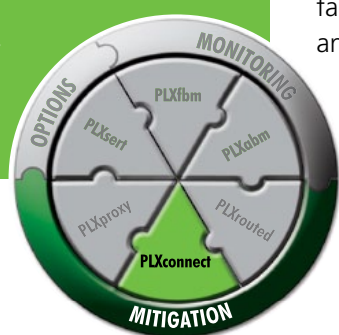
- High bandwidth connectivity for activating Prolexic's on-demand DDoS mitigation services

HOW

- Direct physical connection to Prolexic scrubbing centers via a private cloud

WHY

- High bandwidth — up to 10 Gbps capacity of clean traffic per customer port
- Low impact — no MTU concerns
- Predictable latency — SLA for latency and packet loss





The benefits of Prolexic PLXconnect

Prolexic has developed this service to deliver up to 10 Gbps of clean traffic per customer port – light years ahead of other DoS and DDoS protection providers’ cleanbandwidth capabilities. Today, as denial of service attacks have become extremely large and complex, PLXconnect fulfills a growing need for high capacity and highly reliable direct connectivity. The private cloud eliminates the complex network changes required when using an Internet-based GRE solution. What’s more, we have extended our industry leading SLA to include packet loss and latency guarantees.

Key capabilities

The easiest way to understand PLXconnect is to compare its characteristics and capabilities to routing using GRE.

Characteristic	Generic Route Encapsulation	PLXconnect
Bandwidth	Low	High
Ideal level of application interaction	Simple	Complex
Latency	Unpredictable	Predictable
Encapsulation Overhead	High	Low

Be prepared with PLXconnect

The threat of DDoS attacks continues to escalate – and no business or organization is safe from being the target of malicious cyber criminals. Trust your online presence to Prolexic, the gold standard in DDoS protection services, and rely on the global strength of our PLXconnect Service. Contact us at **+1 (954) 620 6002** or **sales@prolexic.com** to learn how we can protect you against the largest and most complex DoS and DDoS attacks.

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.

DDoS Mitigation: Routed Solution (PLXrouted)

Flexible, asymmetric, on-demand DDoS mitigation

The Routed Solution (PLXrouted) Service Plan is Prolexic's standard DDoS mitigation service platform that provides maximum protection against the broadest range of DoS and DDoS attack types and defends against today's high bandwidth, sustained attacks. PLXrouted DDoS protection is offered as a flexible, asymmetric, on-demand service and enables Prolexic customers to easily activate denial of service attack protection for an entire subnet by redirecting Internet traffic to the Prolexic network during a DDoS attack and routing off of the Prolexic network during non-attack periods.

Why Prolexic PLXrouted DDoS mitigation

You should choose PLXrouted for DDoS protection if you:

- Want more flexibility and efficiency in customizing DDoS denial of service attack protection
- Need to protect a large number of destination IP addresses
- Need a simpler way to activate DDoS protection for an entire subnet
- Are already using BGP at your Internet edge
- Require a resilient solution that facilitates making changes to entire subnets
- Need to protect multiple service types and protocols, not just HTTP and HTTPS
- Are not currently under DoS or DDoS attack – PLXrouted is only available to be deployed for proactive protection

No other company can match Prolexic in what we deliver to our customers every day: the fastest time-to-detect and time-to-mitigate for DoS and DDoS attacks as well as real-time monitoring and response to signature or vector changes – all beginning within minutes of when you redirect your traffic through Prolexic's scrubbing centers.

How Prolexic PLXrouted works

PLXrouted Service Platform relies on standard IP routing protocols to enable Prolexic to on-ramp your incoming traffic and inspect it for anomalies or misbehaviors. Outgoing traffic is not inspected, but allowed to take its normal path. We identify all legitimate traffic and forward it on while silently dropping attack traffic.

PLXrouted uses the GRE (Generic Route Encapsulation) protocol to construct virtual connections to your routers, enabling our routers and yours to "see" each other as directly connected across a tunnel. The BGP routing protocol is used to communicate network advertisements from your site to Prolexic. You use these network advertisements to activate and deactivate the service as needed.

WHAT

- A flexible, asymmetric, on-demand DDoS mitigation service capable of defeating the largest attacks using Prolexic's 1+ Tbps of Internet bandwidth

HOW

- Enables all inbound customer traffic to route through Prolexic
- Provides cost-efficient customization of DDoS protection
- 24/7 remote monitoring at Prolexic's Security Operations Center (SOC)
- Project management expertise to manage complex deployments for large enterprises

WHY

- Provides maximum protection against the broadest range of DDoS attack types
- 24/7 DDoS mitigation backed by the world's leading DDoS experts at Prolexic's SOC
- Fulfills need to protect large numbers of destination IPs
- Provides a simple mechanism to activate DDoS protection for an entire subnet





Activation is complete when Prolexic communicates these advertisements to its upstream carriers and peers from the relevant scrubbing facilities, a process that normally occurs in a few seconds. Traffic is then cleansed and forwarded across the tunnels to the customer's router(s). Over the course of this interception process, outgoing traffic from your servers to the Internet is always forwarded as normal to your ISP(s). This approach, called asymmetric routing, maximizes the benefits of Prolexic's scrubbing process while minimizing the overall impact on your typical traffic flow.

Key capabilities

Capability	Supported
HTTP	Yes
HTTPs	Yes
Other Protocols	Yes
Per-subnet activation	Yes
Per-domain activation	No
Source IP rewritten	No
Symmetric traffic flow	No
Asymmetric traffic flow	Yes
Routers required	Yes

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.

The benefits of Prolexic PLXrouted

Making DDoS denial of service attack protection a tightly integrated part of your network with Prolexic's Routed Solution provides the following benefits:

- **Resiliency** – Route advertisements are propagated from all scrubbing centers
- **Control** – Quick and easy activation/deactivation via simple routing changes enables you to manage your own traffic routing
- **Source IP visibility** – Incoming clean traffic is not modified
- **Improved network security** – No need to "white list" the Prolexic proxy due to source IP visibility
- **Customized DDoS protection** – Prolexic will fine tune and adapt its DDoS attack mitigation and processes based on your individual requirements

PLXrouted DDoS mitigation is further enhanced with the addition of Prolexic's Flow Based Monitoring and state-of-the-art Application Based Monitoring Services.

Be better prepared with Prolexic

Trust your online presence to Prolexic, the gold standard in DDoS attack mitigation services. Contact us at **+1 (954) 620 6002** or **sales@prolexic.com** to learn how we can protect you against the largest and most complex DoS and DDoS attacks.

DDoS Mitigation: Proxy Solution (PLXproxy)

On-demand, symmetric DoS and DDoS protection

Prolexic's Proxy Solution (PLXproxy) is designed to provide rapid Distributed Denial of Service (DDoS) protection for organizations who are under sustained attacks. PLXproxy can restore accessibility to a website brought down by a DDoS attack in just a few minutes after all traffic to the site is routed through Prolexic's global scrubbing centers. Prolexic DDoS mitigation experts identify, analyze and remove the malicious traffic, allowing only the legitimate traffic from your customers and users to flow through. If the attacker randomly changes signatures, our mitigation experts will detect them immediately and take defensive action until all denial of service attack activity ends.

Best of all, activation of PLXproxy DDoS protection is fast and easy with a simple DNS change. In addition, migration to Prolexic's routed solution (PLXrouted) for DDoS mitigation is also simple, if you choose to implement a more robust defense.

WHAT

- An on-demand, symmetric mitigation solution to help those experiencing a DoS or DDoS attack

HOW

- Redirects all inbound and outbound traffic through Prolexic
- Removes malicious traffic while allowing legitimate traffic to flow through
- 24/7 remote monitoring at Prolexic's Security Operations Center (SOC)

WHY

- Rapid DDoS protection when your domain is under attack
- Avoid millions in lost revenue due to site downtime
- Quick activation/deactivation via DNS changes



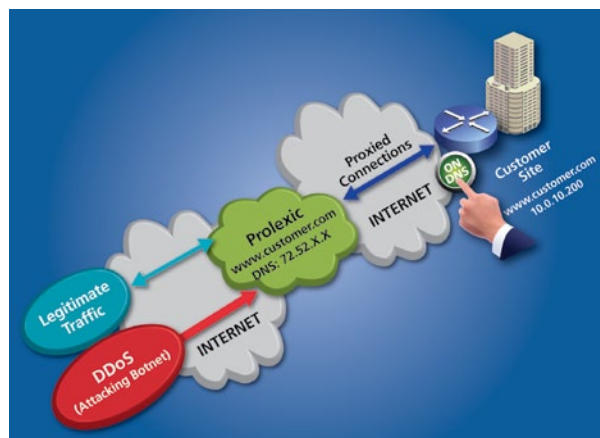
How PLXproxy DDoS protection works

PLXproxy provides rapidly deployed protection against DDoS attacks on the most commonly targeted services. This shared, symmetric, on-demand service enables Prolexic customers to easily activate DDoS protection

per domain and redirect Internet traffic to the Prolexic network during a denial of service attack and then switch off of the Prolexic network during non-attack periods.

Virtual IP addresses (VIPs) are advertised from each of Prolexic's global scrubbing centers. This configuration enables both clean and malicious traffic to be automatically routed to the optimum scrubbing center or centers. Prolexic proactively manages these traffic patterns to optimize the service based upon a general shared profile among all PLXproxy customers.

Prolexic is ready to accept traffic at a moment's notice. Both inbound and outbound traffic flows are directed through Prolexic's scrubbing centers, with Prolexic acting as an intermediary for all communications.



A simple remapping of the IP address associated with a DNS name is all that is required to activate the service. Once activated, traffic will be redirected to the nearest Prolexic scrubbing center for analysis. After malicious traffic is silently discarded, valid traffic is forwarded to your servers.

Mitigation

For all DDoS attacks Prolexic offers a 15-minute time-to-mitigate SLA. For encrypted attacks, Prolexic offers a 20-minute SLA if encryption keys have been uploaded to Prolexic's secure customer portal. Prolexic protects businesses from all types of DDoS attacks regardless of size including, but not limited to: SYN floods and TCP flag abuses, UDP, ICMP, DNS, and HTTP floods as well as HTTPS attacks (if encryption keys are provided).

Key capabilities

Capability	Supported
HTTP	Yes
HTTPS	Yes
Other protocols	No
Per-subnet activation	No
Per-domain activation	Yes
Source IP rewritten as proxied traffic passes through*	Yes
Symmetric traffic flow	Yes
Asymmetric traffic flow	No

*Only possible if Prolexic possesses SSL certificate/key

The benefits of PLXproxy DDoS protection

- **Resiliency** – Prolexic proxies are anycast via all of our scrubbing centers
- **Control** – Quick and easy activation/deactivation via DNS changes enables you to manage your own traffic routing
- **Simplified deployment** – Requires minimal changes to your network environment and can be easily migrated to Prolexic's Routed Solution
- **Emergency rapid deployment** – Fast deployment to enable mitigation of DoS and DDoS attacks in just minutes
- **Minimal impact** – Redirection of the only domain under attack as opposed to an entire subnet
- **CDN optimized** – Tested with the leading CDNs to ensure seamless integration

PLXproxy DDoS protection is further enhanced with the addition of Prolexic's flow based monitoring (PLXfbm) and state-of-the-art application based monitoring services (PLXabm).

Call Prolexic first for fast DDoS mitigation

If your site is attacked or if you want the most robust DDoS protection, call Prolexic, the gold standard in DDoS attack mitigation services. Contact us at **+1 (954) 620 6002** or **sales@prolexic.com** to learn how we can protect you against the largest and most complex DoS and DDoS attacks.

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.

Advanced DDoS Insight Service

Introducing PLXsert

The world of Distributed Denial of Service (DDoS) is constantly changing as new tools, threats and tactics emerge. That's why Prolexic developed PLXsert – a subscription service that provides current threat intelligence, infrastructure and defense evaluation, as well as post attack forensics.

The Prolexic Security Engineering and Response Team (PLXsert)

PLXsert monitors malicious cyber threats globally and analyzes DoS and DDoS attacks using proprietary techniques and equipment. Through digital forensics and post attack analysis, PLXsert is able to build a global view of DDoS denial of service attacks. 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. Formerly an internal research group, PLXsert now provides digital forensics and other services to subscribers.

PLXsert services include:

- **Post-Attack Forensics** – Access Prolexic's post-attack forensic analysis experts for two incidents per year with the option of additional access priced per incident as needed. This service provides in depth analysis of the malware family that generated the attack, expert opinions on the attack, and how it fits into the broader attack landscape.
- **Exclusive Emergency Threat Advisories** – PLXsert customers receive time-sensitive Emergency Threat Advisories that are not released to the public. Information and intelligence contained in these advisories is proprietary and only shared with Prolexic's "inner circle" because it can tip off DDoS perpetrators or potentially hasten attacks. Emergency Threat Advisories may contain information about critical threats or trends in malware that may affect a specific vertical or type of Internet presence.
- **IP Reputational Database Feed** – With the PLXsert subscription service, you can access to a rich data source on global DoS and DDoS threats and activities that Prolexic mitigation technicians compile in their fight against DDoS attackers. As a result, you can make more informed decisions and be more proactive in defending your business against DDoS attacks – both before and after a denial of service attack.

The IP Reputational Database includes a large set of real (non-spoofed) valid source IP addresses observed by Prolexic in DDoS attacks. Provided as a batch file, this information is augmented by geolocation and is continuously updated.

WHAT

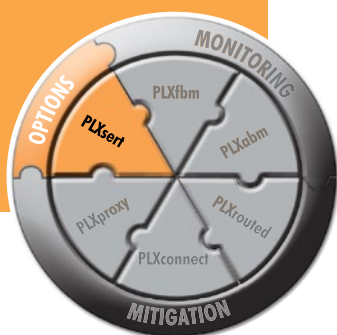
- Subscription service available to Prolexic DDoS mitigation clients that provides pre-and post-attack insight and intelligence on DDoS attacks

HOW

- Monitors and tracks malicious cyber threats globally
- Provides up-to-date intelligence and analysis
- Issues Threat Advisories with remediation recommendations
- Compiles IP Reputational database detailing active botnets

WHY

- Adopt best practices for DDoS mitigation
- Minimize impact of DDoS attacks by taking proactive measures
- Make better, informed decisions on enterprise DDoS protection





> Build an intelligent DDoS defense with PLXsert

Enhance your Prolexic protection with services from PLXsert and build a more intelligent and proactive DDoS defense. Contact us at +1 (954) 620 6002 or sales@prolexic.com to learn how your online business can benefit from the insight and expertise of the PLXsert team.

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 SSL Capabilities

Distributed Denial of Service (DDoS) attacks using the Secure Sockets Layer (SSL) are the most sophisticated DDoS attacks on the Internet. However, even the best DDoS mitigation engineers at Prolexic cannot identify and analyze an encrypted Layer 7 attack without examining packet headers. That's why Prolexic developed the PLXabm SSL Hardware Security Module (HSM) and SSL capabilities for our PLXproxy mitigation service to protect the integrity of your SSL keys at all times. Only Prolexic offers this innovative approach to mitigating DDoS attacks on the SSL layer.

DDoS monitoring for the SSL channel

The PLXabm SSL HSM is compliant with FIPS 140-2 Level 2 key management standards. Built on proprietary Prolexic technology used in our scrubbing centers, the HSM provides a secure way to decrypt SSL traffic so that the PLXabm appliance can be used for SSL attack detection and analysis. The decryption of traffic is performed in hardware on the HSM, but no secure information is ever used in the correlation process. The benefit: the PLXabm HSM keeps your keys and confidential customer information secure, but still allows Prolexic's correlation engine to identify DDoS attacks at the SSL layer.

PLXabm SSL enables our DDoS mitigation engineers to identify and isolate the source IP passively and block encrypted Layer 7 attacks asymmetrically without ever handling or looking at the customer's SSL keys.

How PLXabm SSL works

- Upload your SSL keys to the PLXabm SSL HSM. One way is to use the PLXabm SSL wizard on the secure Prolexic Customer Portal, which uses FIPS 140-2 Level 2 compliant protocols to transfer the keys from the Portal for distribution to the HSMs on all of the PLXabm appliances in your environment. The alternative is to bypass the Portal and upload keys manually on-site using direct import to the HSM itself on each of the PLXabm appliances.
- From the PLXabm SSL module Prolexic runs a client-server authentication from our secure portal that communicates securely from the portal to your data center.
- The PLXabm SSL hardware security module allows for high assurance decryption within the appliance using a separate correlation engine that stores only what is necessary to identify and diagnose DDoS attacks. Confidential information in the payloads, such as credit card data and cookies, are not stored or analyzed in the Prolexic mitigation system.
- We identify and isolate the bot source IPs passively with your secure keys maintaining data integrity, so we can continue to block traffic in our data centers asymmetrically without looking at the SSL channel. This is a highly innovative and different approach to mitigating attacks on the SSL layer that no other DDoS mitigation service provider offers.

AT A GLANCE

What

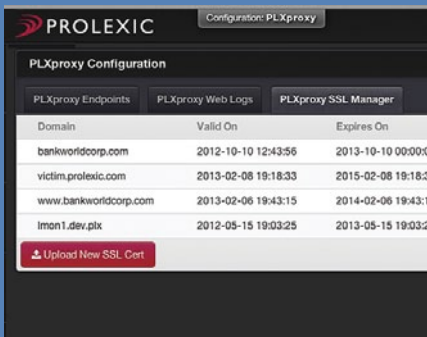
Prolexic's capabilities for mitigating encrypted malicious traffic that uses the Secure Sockets Layer (SSL) data transfer protocol

How

- Passive decrypting of the SSL channel when a DDoS attack is detected (PLXabm)
- Compliant with FIPS-140-2 Level 2 key management standards (PLXabm)
- Active inspection using encryption keys and certificates (PLXproxy)

Why

- Faster identification and isolation of the source IP to block encrypted Layer 7 attacks
- SSL keys are always under the customer's control



Upload and deploy keys with PLXproxy SSL Manager

The PLXproxy SSL manager is an easy-to-use, intuitive wizard for uploading a new SSL certificate into Prolexic's secure internal certificate store. Prolexic's SOC engineers use internal provisioning tools to deploy the certificate out to the proxy servers within Prolexic's infrastructure.

- SSL keys can be deleted manually by submitting a request to the SOC
- Certificates and key pairs are validated and the key is encrypted and stored in a secure "key vault"
- Only the Prolexic API gains access to the key while stored in the key vault, with access limited to SSL inspection and mitigation
- Prolexic audits the entire process to protect against unauthorized access to the SSL key vault

DDoS mitigation for the SSL channel

Prolexic's SSL capabilities within our PLXproxy DDoS mitigation service are backed by a 20-minute time-to-mitigate Service Level Agreement (SLA) if we have access to the encryption keys. If we do not have the keys, the SLA does not apply.

Prolexic employs three different, proven approaches to mitigating encrypted Layer 7 denial of service attacks.

- **SSL attack mitigation with encryption keys** – To monitor an SSL session, Prolexic's DDoS mitigation engineers must see the inbound certificate and key response in order to decrypt the traffic. This requires the customer to upload the keys to Prolexic through the secure portal. The keys are used to decode the traffic, which is analyzed and correlated to develop signatures capable of blocking the malicious traffic. Prolexic stores the keys in an encrypted system that is audited every year to comply with leading industry security practices.
- **SSL attack mitigation without encryption keys** – If we do not have the encryption keys to work within the application, we cannot identify the attack signatures at Layer 7. Without encryption keys, Prolexic can only provide traffic analysis at the network layer, such as measuring connection rates and bit rates per client IP, which opens up greater potential for false positives and collateral damage to the network.
- **SSL attack mitigation with self-signed or temporary certificates and keys** – Prolexic has developed a solution using temporary certificate and key pairs. They are valid only for a short time period to give Prolexic access to the encrypted payload during a DDoS attack, enabling you to retain complete control of the original key and certificate pair. After the DDoS attack is over, you can revoke the certificate and remove the keys from the servers whereby Prolexic loses visibility into the SSL session. The customer's root certificate and keys maintain integrity because Prolexic never had access to anything other than the short-term certificate and key pair.

Strengthen your defense against encrypted DDoS attacks

As attackers develop new toolkits specifically for encrypted Layer 7 attacks, why not leverage Prolexic's SSL detection and analysis capabilities as part of a proactive DDoS defense? After all, Prolexic is the only DDoS mitigation services provider who has successfully mitigated SSL attacks and offers a time-to-mitigate SLA. Contact us to learn more.

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.

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.



Protects hundreds of the world's largest brands

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

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

All resources focused on DDoS mitigation and network protection



“Prolexic is clearly the best DDoS mitigation provider in the industry.”

Andre Bertrand, Security Services Manager, SEEK.com.au

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 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.



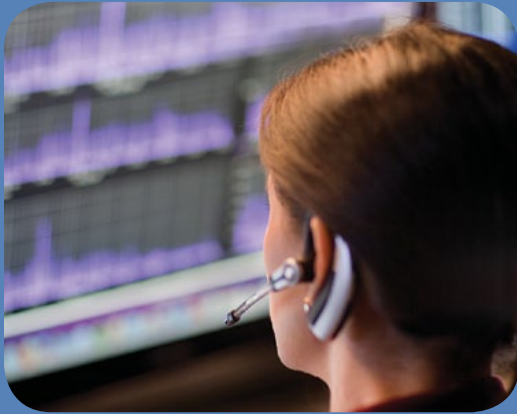
The Prolexic Portal – See what’s happening on your network and ours

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.

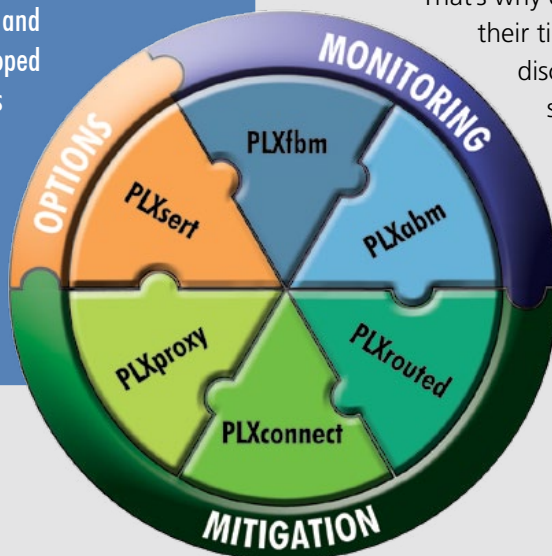
“Yola looked for a best-in-class partner that could maintain service uptime and mitigate all types of DDoS attacks, no matter how large or complex. After reviewing many options, Yola selected Prolexic.”

Lisa Retief, Vice President of Engineering, Yola



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.



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.

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.



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 has done a great job. Having someone you can go to with the knowledge of how to react to issues right away is a big advantage.”

Darin Grey, Chief Technology Officer
Swiss Watch International (worldofwatches.com)

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.