

# Top effective anti-DDoS software

The number of DDoS attacks has increased significantly in scale and complexity, causing business disruption, financial loss and reputational damage. Effective anti-ddos software such as Bizfly Anti DDoS

According to Digit's 2024 report, the number of DDoS attacks has increased significantly in scale and complexity, causing business disruption, financial loss and reputational damage. Many businesses have turned to specialized security solutions to respond. In the following article, TipsMake will introduce to readers the 10 most effective anti-DDoS software today.

## Bizfly Anti DDoS

Bizfly Anti DDoS is a solution against DDoS attacks developed by TipsMake. Bizfly Anti DDoS is a tool that helps businesses protect their websites and landing pages.



Outstanding features:

1. Automatically filter and block DDoS attacks from attack sources in a short time.
2. Capcha mechanism support enhances the system's prevention efficiency when attacked.
3. Does not affect SEO because it does not block access from bots serving SEO.
4. Integrate CDN for HTML data to optimize transmission capacity and increase page loading speed.
5. Web server load balancing based on actual traffic load.
6. Blocks different types of DDoS attacks at IP, application, protocol levels.

## VNIS VNETWORK's anti-DDoS service

VNIS provides anti-DDoS services for game servers, websites, VPS on cloud computing platforms, capable of resisting attacks up to 2600 Tbps. Comprehensive protection system thanks to the integration of many security solutions.

Highlights:

1. Integrate and manage multiple CDNs on one platform, improving website performance, security, and ensuring flexibility.
2. Present in many countries.
3. Traffic filtering and WAF coordination continuously, automatically redirecting when there is a problem.
4. Automatically control and block bad traffic from entering the blacklist.
5. 24/7 operation with professional technical team monitoring and analysis.

## Cloudflare

Cloudflare provides protection against distributed denial of service (DDoS) attacks through a comprehensive, automated system designed to detect and mitigate DDoS attacks across multiple layers of the OSI model, including layers 3, 4, and 7.

Highlights:

1. Use automated DDoS systems to detect and mitigate DDoS attacks without causing latency or impacting performance.
2. Provides protection against multiple types of DDoS attacks on layers 3/4 and 7 of the OSI model. Users can customize mitigation rules to suit their needs.
3. Detect and mitigate sophisticated TCP attacks such as randomized and spoofed ACK floods or SYN and SYN-ACK floods.
4. Protection against DDoS-based DNS attacks, including both random and complex attacks.

## Radware

Radware provides cloud-based DDoS protection for enterprises and service providers, with security capabilities for Private Cloud, Public Cloud, and 5G infrastructure for large-scale networks.

Highlights:

1. Detect and mitigate multi-vector attacks, protecting against complex network and application attacks.
2. Use machine learning algorithms to distinguish between legitimate and attack traffic.
3. Real-time signature generation against new and unknown attacks.
4. Integrated Web Application Firewall (WAF) protects web applications from attacks like Slowloris and dynamic flooding.
5. Supports multiple deployment methods, including cloud and dedicated appliances.
6. Emergency Response Team (ERT) support 24/7.

## Akamai Prolexic Routed

Akamai Prolexic Routed is an advanced Distributed Denial of Service (DDoS) protection service designed to stop DDoS attacks before they reach your applications, data centers, and infrastructure.

Highlights:

1. Capable of preventing many common attacks such as UDP floods, SYN floods, and HTTP GET/POST attacks.
2. Helps maintain high performance and stability for your system by minimizing latency and enhancing network resiliency.
3. Offers flexible deployment options, including always-on and on-demand, giving you greater control over your mitigation posture.
4. Get industry-leading DDoS mitigation expertise, allowing you to focus on your business without disruption

## **AWS Shield**

AWS Shield is a DDoS protection solution that monitors traffic to servers to detect and handle malicious traffic. It uses measures such as packet filtering and traffic prioritization.

Administrators can use AWS WAF to write application-layer attack protection rules. AWS Shield Advanced provides advanced protection, mitigating the impact of large DDoS attacks.

Highlights:

1. Provides automated DDoS mitigation at the application layer (L7), requiring no manual intervention from you or AWS SRT.
2. Seamlessly integrates with essential AWS services like AWS WAF, Amazon CloudFront, and Amazon Route 53, providing a comprehensive security framework.
3. Early detection of DDoS attacks, timely notification via Amazon CloudWatch

## **Sucuri Website Firewall**

Sucuri is a website security company that provides solutions to protect websites from cyber attacks, including DDoS attacks. Their cloud-based service helps prevent hacker attacks and increase website security.

Highlights:

1. Web application firewalls help prevent DDoS attacks and zero-day exploits, thoroughly inspect all HTTP/HTTPS traffic entering a website, and block suspicious requests.
2. DDoS and Geo-Blocking Block access from areas at high risk of DDoS attacks.
3. CDN (Content Delivery Network) is available to reduce network traffic and increase website performance.

## **Imperva DDoS**

Imperva's DDoS protection solution is designed to protect businesses from distributed denial of service (DDoS) attacks by blocking malicious traffic at the endpoint, ensuring continuous operations without impacting performance.

Outstanding features

1. Protect your business assets, whether on premises or in the cloud.

2. Block malicious traffic to applications, protecting businesses from large-scale DDoS attacks.
3. Providing application security, API security and microservices solutions.
4. Use machine learning to detect attack patterns and stop large-scale campaigns.
5. Mitigate risks from third-party JavaScript and prevent client-side attacks like data theft and digital identity theft.

## Link11

Link11 develops cloud computing security solutions against DDoS attacks for websites and IT infrastructure. Using AI to automatically filter malicious traffic, the company provides 24/7 support in Europe and quickly sets up security systems for new customers, helping them respond promptly to attacks.

Highlights:

1. Anti DDoS website.
2. CDN load balancing.
3. Provide threat intelligence.
4. Bot Management.
5. WAF prevents attacks exploiting Zero-day vulnerabilities.

You finished reading the article "**Top effective anti-DDoS software**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.