

ARBOR CLOUD

Pros

As an established brand, Arbor not only offers cloud-based and on-site protection services, but it also lends its hardware to other DDoS mitigation services.

Cons

This service provider does not offer a web application firewall.

The Verdict: 9.05/10

While Arbor does not feature a web application firewall, the service uses specialized software and internal counter measures to block DDoS attacks.



What We Do

Arbor Networks helps secure the largest enterprises and provider networks from DDoS and advanced attacks.

Global Traffic Intelligence

ATLAS is a collaborative project with more than 330+ ISP customers who share 120 Tbps of traffic data.

With this global insight, Arbor is ideally positioned to deliver intelligence about, and protections for, DDoS, malware and botnets that threaten enterprise networks.

Network Visibility

Global traffic intelligence together with NetFlow and Packet Capture technology to help customers see and understand what is happening across their network, no matter its size.

Improve network operations and security by quickly identifying service and performance issues, traffic anomalies, malicious insiders and unauthorized use.

DDoS Protection

On-premises appliances, cloud, hybrid, network-embedded and virtual DDoS protection solutions for organizations of all sizes and industries.

Ensure the availability of your critical infrastructure with the world's most proven, broadly deployed DDoS mitigation technology.

Advanced Threat Solutions

Powerful security analytics, real-time and historical traffic intelligence and data visualizations bring meaningful security context to massive amounts of data, transforming threat detection and incident response.

See and respond to the most serious advanced attacks on the network faster and with more detail than ever before.



Arbor Networks is one of the largest DDoS mitigation services. The company not only offers advanced mitigation techniques, but it also is in the unique position of providing its hardware to several of its competitors. Arbor Cloud offers a unique combination of on-premise and cloud-based mitigation techniques to thwart even the most sophisticated DDoS attacks.

Between the advanced hardware, specialized software and multiple, large-scale scrubbing centers, this DDoS protection service is designed to stymie stealthy attacks. We've given Arbor our Top Ten Reviews Bronze Award for its various mitigation tools and the advanced technology it offers to help defend against DDoS attacks.

Infrastructure

8/10

With four data centers spread across the world and more being constructed, Arbor is prepared for large-scale volumetric attacks with a vast amount of available network capacity. This DDoS service has a network capacity of 1.14TB and a scrubbing capacity of 1.14TB. Three of its scrubbing centers operate at 320GB per second, while one of them operates at 180GB per second. At this rate, the service offers deep packet inspection to verify data is clean while not frustrating or sending away visitors of your website due to slow loading times.

Arbor Cloud does not use a firewall since they are susceptible to DDoS attacks. Instead, the company uses proprietary software designed to block attacks as well as internal counter measures. For example, one such countermeasure is a challenge, like CAPTCHA, to determine if traffic is genuine or malicious. It also automatically differentiates bad bots from humans and good bots by identifying the telltale, distinguishing behaviors of malicious traffic.

Arbor also uses standard mitigation techniques like rate limiting, IP blocking and border gate protocol to identify and mitigate various forms of DDoS attacks. The service also uses real-time monitoring to observe traffic and alert you to suspicious activity.

Deployment & Protection Methods

10/10

Arbor offers on-site, hybrid and cloud-based deployment. The hybrid model has always-on protection with its multi-layer deployment mod-

el. This model offers on-premise protection with a prevail availability protection system device that sits on the edge of the network and alerts you to DDoS attacks. This device is customized to the client's network and analyzes and routes traffic. If it catches suspicious traffic, it immediately sends a signal to cloud deployment to route traffic to a safe zone. You can set up the on-premise device to automatically or manually alert the cloud to a DDoS attack. After a certain threshold, you can preset the device to automatically signal to the cloud, or you can manually signal the cloud when you think an attack is underway.

Arbor customizes its services to customers' needs and networks, giving you the protection best suited for your site. The company offers unlimited mitigation against DDoS attacks. You can opt for either on-demand or always-on protection. The company suggests using on-demand protection, since always on can unnecessarily route and slow down your traffic, which could have a negative impact on end users.

Management Options

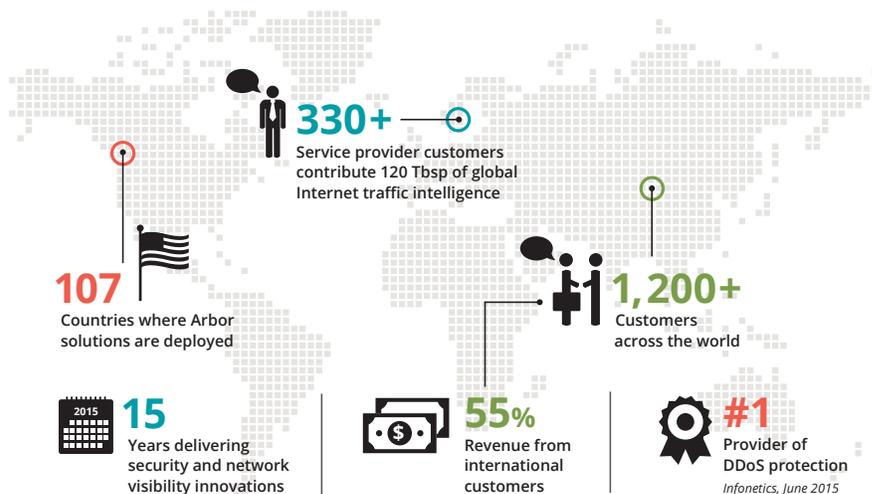
10/10

Arbor offers a centralized management dashboard you can access after you become a client. It provides timely reports regarding traffic and security reports, weekly briefs and more. Clients can generate reports, but they cannot configure the settings.

ARBOR
NETWORKS
The Security Division of NETSCOUT

DDoS and Advanced Threat Protection for Enterprise and Service Provider Networks. Backed by global traffic intelligence into emerging threats.

By the Numbers



Help & Support

8.5/10

Like other DDoS mitigation services, Arbor offers a service level agreement spelling out the specific services it stands behind, including 24-hour monitoring. If needed, you can pay more for a dedicated support manager to monitor the security of your site. If you need to contact the company, you can reach them via email and a toll free number listed on Arbor's website. They also list an emergency toll-free phone number to call during DDoS attacks.

Arbor Summary:

9.1/10

Arbor uses a dual approach to fighting DDoS attacks by integrating cloud-based and on-premise protection into one application. This hybrid approach can be very useful when guarding against certain forms of DDoS attacks, such as application-layer attacks, that are better detected and mitigated on premise versus other forms of attacks, such as flood attacks, that can be neutralized using cloud-based techniques. This DDoS service provider does not offer a firewall, but as one of the largest DDoS mitigation services, you can rely on the vast resources Arbor uses to protect your site from attacks of all sizes.

