KNOWLEDGE BRIEF

Arbor Networks is Recognized as the 2017 Market and Technology Leader in the Global DDoS Mitigation Market

KNOWLEDGE BRIEF

BY

Quadrant
Knowledge Solutions

Arbor Networks is Recognized as the 2017 Market and Technology Leader in the Global DDoS Mitigation Market

Distributed Denial of Service (DDoS) attacks are targeted attacks against specific company, to make the network, server, web application or services unavailable to its users. DDoS attacks are often carried out to interrupt business operations and disturb communications. This results in network downtime and can cause significant damage to organizations in terms of lost opportunities, information theft and damage to its brand value. For industries that mostly rely on their online presence for businesses, such as eCommerce, online payment, online gaming, and others, DDoS attacks can result in huge losses.

DDoS Mitigation is a technique to secure company's network against DDoS attacks on systems connected to the internet by ensuring protection on targeted networks. This is achieved by passing system activity targeted to the attacked system through high-limit systems with filter channels. DDoS mitigation requires an effectively distinguishing approach to a particular human activity from fake bots and captured web programs. The procedure is done by considering encrypted signatures and inspecting distinctive characteristics of the incoming traffic, including IP addresses, Javascript impressions, and various HTML headers.

DDoS Mitigation market has presence of suppliers of DDoS appliances as well as service providers. Modern DDoS mitigation appliances are capable of providing mitigation up to 40 Gbps of attacks and by combining these appliances, it handles multiple of hundreds of attack volume capacity. On the other hand, DDoS mitigation service providers use multiple high capacity scrubbing centers and can handle Tbps of attack volume capacity. Most of the large organizations are looking at deploying hybrid solutions by investing in both on-premise appliances as well as cloud-based DDoS mitigation services. DDoS mitigation suppliers continue to collaborate in providing integrated hybrid-based solutions.

Quadrant Knowledge Solutions' recent study of the "***DDoS Mitigation Global Market Outlook***" analyzes market dynamics, opportunities and the competitive vendor landscape of the market. This study provides strategic analysis of the global DDoS Mitigation market in terms of short-term and long-term growth opportunities. The study also provides detailed market forecast analysis of the global market in various geographical regions, revenue types, customer types, industry segments, and sales channel. The DDoS Mitigation market outlook research helps companies formulate growth strategies by identifying growth prospects, market trends, market drivers, and challenges in the global market.

The research also provides detailed competitive positioning and supplier landscape analysis of major DDoS Mitigation vendors, including A10 Networks, Akamai, Arbor Networks, CloudFlare, Corero, Fortinet, Huawei, Imperva, Nexusguard, NSFOCUS, Radware, and Verisign.

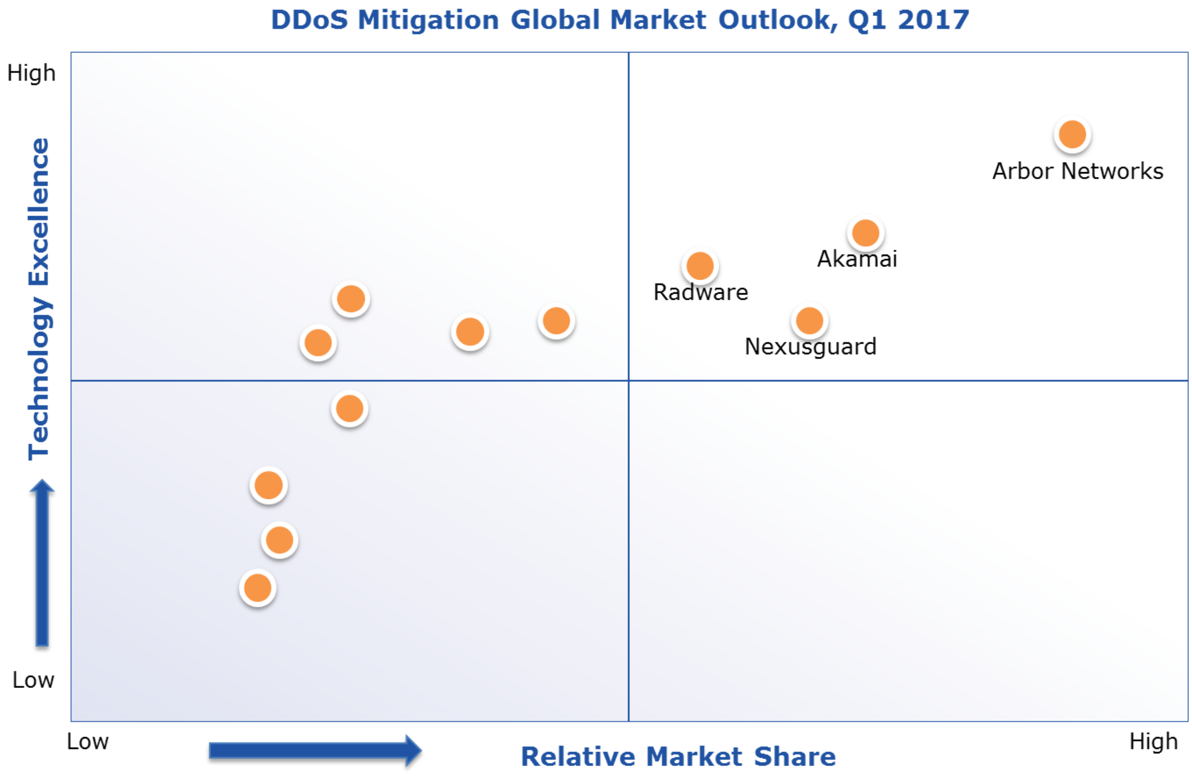
Arbor Networks is Recognized as the 2017 Market and Technology Leader in the Global DDoS Mitigation Market

As part of the research on "DDoS Mitigation Global Market Outlook," Quadrant's competitive landscape analysis compares vendors' technological capabilities in providing DDoS mitigation solutions. Quadrant research analyzed vendors in terms of business performance and technology excellence parameters. According to the research findings, Arbor Networks is recognized as the market and technology leader in the global DDoS mitigation market driven by its sophistication of technology platform, scalability, competitive strategy, industry impact, and high customer impact.

Founded in 2000, Arbor Networks is the market leader in the global DDoS mitigation market. The company with its innovative DDoS mitigation solution backed by its global threat intelligence service is the most popular DDoS mitigation provider amongst larger tier-1 service providers and large enterprises. Arbor Networks, with over 1,200 customers in 107 countries, is well recognized for its innovative multi-layered DDoS mitigation solution including APS appliance, Cloud Signaling^{TM}, Arbor Cloud, Arbor Networks TMS, and network visibility products.

According to Piyush Dewangan, Industry Research Manager, Quadrant Knowledge Solutions, "DDoS attacks are growing in numbers, sophistication, and complexities; and hence emerging as the largest security threats for securing organizations network." "Most of the modern day attacks are carried out using multi-vector attacks which consists of combination of various attack types, such as volumetric, protocol, and application layer attacks. The multi-vector approach of DDoS attack campaign has very high chances of success as they target different network resources and target infrastructure, applications and services simultaneously. In most of the cases, attacker uses one attack vector as a trap and uses the other most powerful vector as the main weapon for DDoS attack" adds Dewangan.

For effective protection against the complex and multi-vector DDoS attacks, users are increasingly looking at adopting multi-layered hybrid approach by investing in DDoS appliances as well as utilizing the cloud-based DDoS protection services. In this case, during large-volume attacks, user can preset the value and accordingly, can route the traffic to the cloud-based scrubbing services on exceeding its preset value. The increasing trend towards hybrid model is resulting in collaboration and partnership amongst DDoS appliance and cloud-based service providers for integrated hybrid-based DDoS mitigation solution. Arbor Networks, with the introduction of Arbor Cloud along with Cloud Signaling^{TM} feature, offers tightly integrated multi-layered protection capable of mitigating most complex and large scale DDoS attacks.



Arbor Networks Capability in the Global DDoS Mitigation Market

Arbor Networks' comprehensive DDoS mitigation solution portfolio includes its industry leading on-premise appliance Arbor APS, Arbor Cloud for integrated multi-layer defense, and Arbor Networks TMS for carrier-class scrubbing centers. The company's DDoS protection solution products are backed up by ATLAS$^{®}$ global threat intelligence for real-time updates on advanced threats and DDoS attacks.

- **Arbor Networks APS**: Arbor Networks APS is an on-premise appliance which helps protect businesses against the most advanced and sophisticated DDoS attacks including volumetric, protocol and application layer attacks. The Arbor APS appliance is designed to automatically neutralize IPv4 and IPv6 attacks before they harm critical applications and services. Arbor APS uses Cloud Signaling^{TM} to connect local protection with cloud-based DDoS services thereby enhancing protection against the large volumetric attacks. Cloud Signaling^{TM} enables Arbor APS to automatically alert upstream service providers, such as Arbor Cloud or those offered by more than 60 ISPs who leverage Arbor technology as part of their DDoS managed service. This automated connection enables faster time to mitigate larger DDoS attacks. Arbor Networks also offers virtual version of the APS appliance called vAPS that supports VMware and KVM hypervisors. Arbor APS options range from 100 Mbps virtual solutions up to 40Gbps appliances. The company also offers managed APS (mAPS) services suitable for SMBs and large organizations which often lacks expertize and face capital investment challenges. Managed DDoS mitigation service ensures that organization's bandwidth speed is up all the time, and ensures DDoS protection when bandwidth or traffic level increases over the time.

- **Arbor Cloud:** In addition to on-premise APS appliance, Arbor Networks offers Arbor Cloud services to protect enterprises from the full spectrum of today's DDoS attacks. While Arbor APS appliance can detect and provide mitigation of over 40 GBPS of DDoS attack traffic, Arbor Cloud uses multiple high capacity scrubbing centers and can handle multi-Tbps of attack volume capacity. Arbor Networks cloud-based scrubbing services are tightly integrated with the Arbor APS on-premise appliance. With a powerful feature called "Cloud Signaling^{TM}", the Arbor APS can automatically notify and reroute attack traffic to an Arbor Cloud scrubbing center where attacks are mitigated. This multi-layered approach to DDoS protection with the combination of on-premise Arbor APS, Cloud Signaling, and Arbor Cloud, helps enterprises in mitigating the most complex multi-layered DDoS attacks without interrupting enterprise applications and services.
- **Arbor Networks TMS:** Arbor Networks TMS DDoS protection solution is amongst the most popular solution for service providers, cloud providers and large enterprises. Arbor Networks TMS surgically removes DDoS attack traffic from enterprise network without interrupting the flow of non-attack business traffic. It also provides comprehensive real-time visibility into network applications and proactively monitors DDoS attacks for maintaining continuity of network service performance. Arbor Networks TMS is the proven solution in protecting enterprise network or helping service providers to protect their customers from the largest and the most complex volumetric, protocol and application layer DDoS attacks. Arbor TMS automatically detects and surgically removes up to 160 Gbps of DDoS attack traffic from a single appliance and can provide up to 8 Tbps of DDoS attack mitigation capacity from a single deployment. Its flexible and scalable architecture

makes it an ideal solution for in-cloud deployment and the delivery of managed services. TMS solution comes with multiple capacities including 2U appliances (500 Mbps-160 Gbps of mitigation), 6U chassis (10-100 Gbps of mitigation) and Cisco ASR9K Router embedded (10-60 Gbps of mitigation).

- **ATLAS® Intelligence Feed (AIF):** Arbor solutions provide customers with a micro view of their network combined with a macro view of the global internet traffic via the ATLAS threat intelligence infrastructure, making it a powerful combination of network security intelligence. Arbor Networks DDoS protection portfolio of products and services is further enhanced by the ATLAS® Intelligence Feed (AIF) service from the Arbor Security Engineering and Response Team (ASERT). AIF provides real-time updates with actionable intelligence on DDoS attacks and advanced threat campaigns. As Arbor's research team discovers new attack information, the AIF is updated, and changes are delivered automatically to Arbor products via a subscription over a secured SSL connection. With AIF, Arbor Networks is able to provide most up-to-date threat intelligence to its customers with support from a dedicated team of experts adding 'human intelligence' aspect to the threat analysis. By leveraging ATLAS® Intelligence, Arbor customers can make informed decisions about network security as well as service creation, market analysis, capacity planning and application trends. ATLAS® is a collaborative project with over 330 service provider customers who have agreed to share anonymous traffic data consisting of 140 Tbps or approximately one third of all internet traffic.

Last Word

Driven by growing complexities, scale and frequency of attacks, choosing a DDoS mitigation solution has become a must for securing an organization's network and ensuring its availability. Latest trends from security reports of various DDoS Mitigation solution providers suggest that the mega attacks are getting bigger in size and increasingly becoming complex. According to Arbor Networks 12th Annual Worldwide Infrastructure Security Report (WISR), the company reported 800 Gbps as the largest DDoS attack size with other mega attacks of 600 Gbps, 550 Gbps and 500 Gbps. These attacks have the capability to bring the organization's server down within a few minutes of attack. These large scale mega attacks are expected to continue to evolve and can exhaust the bandwidth capacity of the largest enterprise companies. Quadrant Knowledge Solutions recommends organizations for detailed assessment of their network with vulnerability analysis against possible DDoS attacks. This helps organizations in identifying loopholes and vulnerability for possible DDoS attacks. While sometimes initial investments may seem unnecessary or costly, the actual cost after DDoS attacks can be much higher compared to the cost of DDoS Mitigation solutions.

Arbor Networks, with its market leading DDoS mitigation solution is well positioned to help enterprise and service provider companies in ensuring protection against the most complex attacks, both known and unknown. Driven by its innovative technology capability and proven track records, Quadrant Knowledge Solutions recognize Arbor Networks as the 2017 Market and Technology Leader in the Global DDoS Mitigation market.