

DDoS Prevention Appliance Report Excerpts

By **Jeff Wilson**
Principal Analyst, Security
Infonetics Research

The following excerpts are from Infonetics Research's DDoS Prevention Appliances report, reprinted with permission by Arbor Networks.

MOBILE NETWORK AND DATA CENTER SPENDING DRIVING DDoS APPLIANCE GROWTH

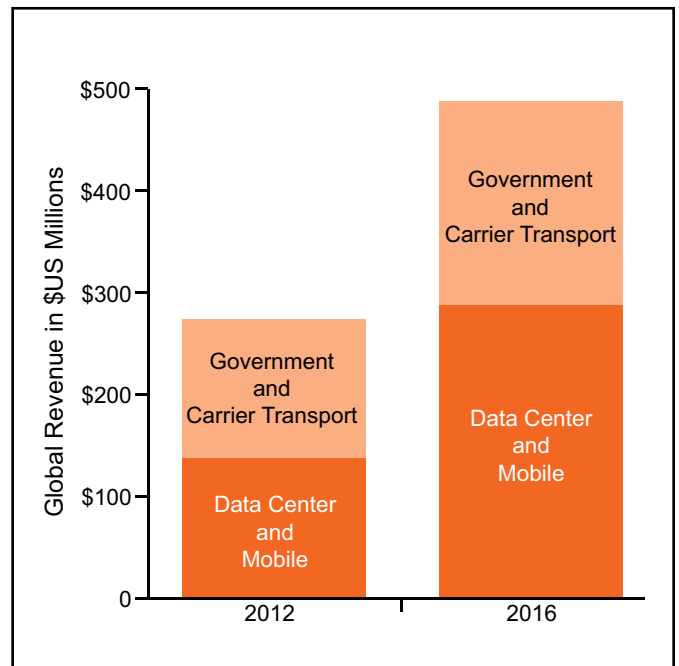
Distributed denial-of-service (DDoS) prevention appliances are the first line of defense for most service providers and large enterprises looking to protect themselves from brute-force attacks on network or resource availability.

With the unprecedented number, size, and coverage of DDoS attacks over the last 24 months (punctuated by a very deliberate set of attacks aimed at US financial institutions in September), vendors who build DDoS prevention solutions have seen and continue to see a significant increase in demand. 2011 revenue was US\$210.6 million, up 43% over 2010, and 2012 worldwide revenue finished at close to US\$275 million, which is nearly 30% above 2011.

Until 2011, the traditional carrier transport market—which Arbor Networks has dominated for nearly a decade—was the largest DDoS deployment location, but it was surpassed by the data center (enterprise and carrier, including hosted DDoS service environments) in 2012.

Going forward, we expect serious activity in the data center segment, which will see a healthy 22% 2011 to 2016 compound annual growth rate (CAGR), versus 9% for the mature carrier transport market.

Forecast: Global DDoS Prevention Appliance Revenue by Deployment Location



Source: Infonetics Research, *DDoS Prevention Appliances*, December 2012

“Arbor Networks dominates the traditional carrier transport segment, has significant revenue share in the data center segment (60.6%), and is gaining ground on the mobile side too.”

JEFF WILSON, PRINCIPAL ANALYST, SECURITY, INFONETICS RESEARCH

The mobile segment shows the most explosive growth (32.7% CAGR from 2011 to 2016) as it rides the compound wave of a transition to IP and data, massive increases in capacity, and a new role as a juicy and highly visible target for attacks. Mobile carriers are interested in protecting their networks and understanding what’s flowing across them, driving many to look at a combination of DDoS and standalone DPI solutions. Arbor alone announced mobile deployments at SK Telecom, Hunan Mobile, and Star Hub in the last 6 months.

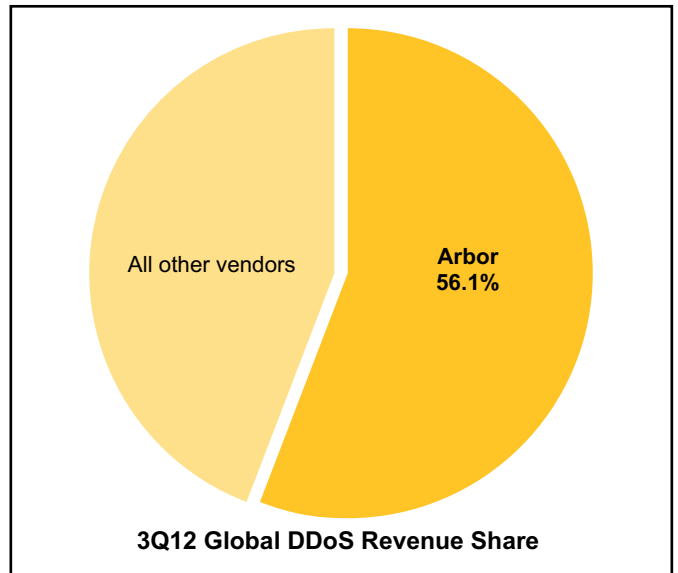
ARBOR IN THE DRIVER’S SEAT

In total third quarter 2012 (3Q12) DDoS prevention appliance revenue, Arbor ranks first with 56.1%, followed by Radware at 8.9% and Narus at 7.1%, respectively. GenieNRM and Andrisoft round out fourth and fifth with 3.1% and 0.3%, respectively.

Arbor leads the market overall, though they lead by slightly less when we look beyond the carrier transport sub-market, which they dominate with over 75% revenue share. They have significant revenue share in data center (60.6%), and addressed a product hole with the release of their Pravail APS solution, but several other vendors have a strong focus on data center and good share position in that segment. Arbor is gaining ground on the mobile side too; their 2010 share of 29.8% grew to 47.2% in 2011, and averaged over 50% in 2012.

With a strong position in the traditional carrier transport market and strong growing share in the fastest growing segments, Arbor is in a strong position to maintain their leading DDoS prevention share position indefinitely.

Arbor Networks leads the overall DDoS prevention appliance market with over half of worldwide revenue



Source: Infonetics Research, *DDoS Prevention Appliances*, December 2012

Infonetics Research forecasts the global DDoS prevention appliance market to reach nearly US\$500 million in 2016.

LONG-TERM DDoS APPLIANCE MARKET DRIVERS

Though there's talk of DDoS integrated into other infrastructure products and cloud-based or hosted DDoS prevention services, the sheer scale of the problem necessitates a high performance, dedicated, appliance-based solution. We believe the following drivers will help push the market to nearly \$500 million annually in 2016:

- The increasing volume of **highly visible attacks**, including a mix of politically motivated attacks, state-sponsored electronic warfare, social activism, organized crime, and good old fashioned pointless mischief and mayhem, driven by the easy availability of bots/botnets for hire and easily distributed crowd-sourced attack tools (like LOIC, originally created by Anonymous to attack the Church of Scientology)
- **Internet traffic growth**, which has driven major carriers to upgrade their backbone infrastructure to increase capacity, driving a need for higher capacity DDoS prevention solutions
- **Enterprise demand** for DDoS prevention solutions, either fulfilled by rolling out their own protection infrastructure, or buying managed services from providers who consume prevention solutions and build services for the end customer
- **Data center consolidation**, data center upgrades, and the rollout of the cloud infrastructure that will underpin the next generation of cloud services; large data centers and cloud providers are highly visible targets who must protect their own infrastructure and the customers who trust them to host data and applications
- **Mobile network upgrades**, which many mobile providers are making to deliver 3G and 4G services and meet the demand for broadband data for mobile devices, are forcing providers to add new layers of network protection and increase their overall security processing capacity; backhaul networks alone are adding orders of magnitude more capacity, driving the need for new DDoS solutions
- **Managed DDoS mitigation services**; in addition to purchasing DDoS solutions to protect their own infrastructure, many carriers around the globe are buying DDoS products to build out managed services for their customers, and specialized hosted DDoS service providers (like Prolexic) are gaining popularity with enterprise customers looking for DDoS prevention but lacking the expertise or capital to deploy their own

DDoS REPORT AUTHOR

Jeff Wilson: Principal Analyst, Security | jeff@infonetics.com | +1 (408) 583.3337 | twitter.com/SecurityJeff

ABOUT INFONETICS RESEARCH

Infonetics Research is an international market research and consulting firm serving the communications industry since 1990. A leader in defining and tracking emerging technologies in all world regions, Infonetics' analysts help clients plan, strategize, and compete more effectively.

SERVICES

- Market Share, Market Size, and Forecasts
- Enterprise/SMB and Service Provider Survey Research
- Continuous Research Services
- Service Provider Capex and Subscriber Analysis and Forecasts
- Consulting, Retainers, and Quick Consults
- Webinar, Conference, and Event Speaking
- Custom Brand and Demand-Side Market Research
- Custom Market Size and Forecasts
- Technology and White Papers
- Competitive Analysis and Due Diligence

COVERAGE AREAS

- Mobile and Wireless
- Small Cells and Carrier WiFi
- Mobile Backhaul and Microwave
- Service Provider VoIP and IMS
- Broadband Access
- Pay TV
- Service Enablement and Subscriber Intelligence
- Carrier Routing, Switching, and Ethernet
- Optical
- Networking Ports
- Vendor Services and Outsourcing
- Service Provider Capex and Subscribers
- Data Center and Cloud
- Security
- Enterprise Networks
- Enterprise Voice, Video, and Unified Communications
- Equipment Vendor Scorecards
- Overall Market Trends and Forecasts

SALES

Interested in distributing excerpts from Infonetics Research's reports? Please contact:

- **North America (West), Asia, Latin America:** Larry Howard, larry@infonetics.com, +1 408-583-3335
- **North America (East), Texas, Midwest:** Scott Coyne, scott@infonetics.com, +1 408-583-3395
- **Europe, Middle East, Africa:** George Stojisavljevic, george@infonetics.com, +44 755-488-1623
- **Japan, South Korea, China, Taiwan:** <http://www.infonetics.com/contact.asp>